

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-06-26.1 | 26 июня 2024 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-33620	Fsas Technologies ID Link Manager и FUJITSU Software TIME CREATOR	Сетевой	RLF	2024-06-18	✓
2	Высокая	CVE-2024-23934	Sony XAV-AX5500	Сетевой	ACE	2024-06-24	✓
3	Критическая	CVE-2024-27174	Toshiba Tec MFPs	Сетевой	RLF	2024-06-21	✓
4	Критическая	CVE-2024-27173	Toshiba Tec MFPs	Сетевой	RLF	2024-06-21	✓
5	Критическая	CVE-2024-27145	Toshiba Tec MFPs	Сетевой	RLF	2024-06-21	✓
6	Критическая	CVE-2024-27144	Toshiba Tec MFPs	Сетевой	RLF	2024-06-21	✓
7	Высокая	CVE-2023-45288	Service Interconnect 1.5	Сетевой	DoS	2024-06-21	✓
8	Критическая	CVE-2024-27174	Toshiba Tec MFPs	Сетевой	RLF	2024-06-20	✓
9	Критическая	CVE-2024-27173	Toshiba Tec MFPs	Сетевой	RLF	2024-06-20	✓
10	Критическая	CVE-2024-27145	Toshiba Tec MFPs	Сетевой	RLF	2024-06-20	✓
11	Критическая	CVE-2024-27144	Toshiba Tec MFPs	Сетевой	RLF	2024-06-20	✓
12	Высокая	CVE-2024-27155	Toshiba Tec MFPs	Локальный	ACE	2024-06-20	✓
13	Высокая	CVE-2024-3498	Toshiba Tec MFPs	Локальный	ACE	2024-06-20	✓

14	Критическая	CVE-2024-27143	Toshiba Tec MFPs	Сетевой	ACE	2024-06-20	✓
15	Высокая	CVE-2024-3497	Toshiba Tec MFPs	Смежная сеть	RLF	2024-06-20	✓
16	Высокая	CVE-2024-3496	Toshiba Tec MFPs	Смежная сеть	OSI	2024-06-20	✓
17	Критическая	CVE-2024-27172	Toshiba Tec MFPs	Сетевой	ACE	2024-06-20	✓
18	Высокая	CVE-2024-27169	Toshiba Tec MFPs	Локальный	SB	2024-06-20	✓
19	Высокая	CVE-2024-27165	Toshiba Tec MFPs	Локальный	ACE	2024-06-20	✓
20	Высокая	CVE-2024-6103	Microsoft Edge	Сетевой	ACE	2024-06-21	✓
21	Высокая	CVE-2024-6101	Microsoft Edge	Сетевой	OSI	2024-06-21	✓
22	Высокая	CVE-2024-6102	Microsoft Edge	Сетевой	ACE	2024-06-21	✓
23	Высокая	CVE-2024-6100	Microsoft Edge	Сетевой	ACE	2024-06-21	✓
24	Высокая	CVE-2024-37081	VMware vCenter Server	Локальный	PE	2024-06-18	✓
25	Критическая	CVE-2024-37080	VMware vCenter Server	Сетевой	ACE	2024-06-18	✓
26	Критическая	CVE-2024-37079	VMware vCenter Server	Сетевой	ACE	2024-06-18	✓
27	Высокая	CVE-2024-36999	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✗
28	Высокая	CVE-2024-23159	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✗

29	Высокая	CVE-2024-23158	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
30	Высокая	CVE-2024-23157	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
31	Высокая	CVE-2024-23156	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
32	Высокая	CVE-2024-23155	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
33	Высокая	CVE-2024-23154	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
34	Высокая	CVE-2024-23151	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
35	Высокая	CVE-2024-23150	Autodesk AutoCAD products	Локальный	ACE	2024-06-19	✘
36	Высокая	CVE-2024-6103	Google Chrome	Сетевой	ACE	2024-06-18	✔
37	Высокая	CVE-2024-6102	Google Chrome	Сетевой	ACE	2024-06-18	✔
38	Высокая	CVE-2024-6101	Google Chrome	Сетевой	OSI	2024-06-18	✔
39	Высокая	CVE-2024-6100	Google Chrome	Сетевой	ACE	2024-06-18	✔
40	Высокая	CVE-2024-5924	Dropbox Desktop	Сетевой	ACE	2024-06-18	✘
41	Высокая	CVE-2022-48622	Gnome gdk-pixbuf	Локальный	ACE	2024-06-18	✔

Краткое описание: Чтение локальных файлов в Fsas Technologies ID Link Manager и FUJITSU Software TIME CREATOR

Идентификатор уязвимости: CVE-2024-33620

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: FUJITSU Software:

FUJITSU Business Application ID Link Manager II: версии 1.8

FUJITSU Software ID Link Manager: версии 2.0

FUJITSU Software TIME CREATOR ID Link Manager: с версии 2.3.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- <http://jvn.jp/en/jp/JVN65171386/index.html>
- <http://www.fujitsu.com/jp/group/fsas/about/resources/security/2024/0617.html>

Краткое описание: Выполнение произвольного кода в Sony XAV-AX5500

Идентификатор уязвимости: CVE-2024-23934

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: XAV-AX5500: до версии 2.00

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

2 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-24 / 2024-06-24

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-875/>

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27174

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии
e-STUDIO 2521AC FC-2521AC: все версии
e-STUDIO 2020AC FC-2020AC: все версии
e-STUDIO 2520AC FC-2520AC: все версии
e-STUDIO 2025NC FC-2025AC: все версии
e-STUDIO 2525AC FC-2525AC: все версии
e-STUDIO 3025AC FC-3025AC: все версии
e-STUDIO 3525AC FC-3525AC: все версии
e-STUDIO 3525ACG FC-3525ACG: все версии
e-STUDIO 4525AC FC-4525AC: все версии
e-STUDIO 4525ACG FC-4525ACG: все версии
e-STUDIO 5525AC FC-5525AC: все версии
e-STUDIO 5525ACG FC-5525ACG: все версии
e-STUDIO 6525AC FC-6525AC: все версии
e-STUDIO 6525ACG FC-6525ACG: все версии
e-STUDIO 2528A DP-2528A: все версии
e-STUDIO 3028A DP-3028A: все версии
e-STUDIO 3528A DP-3528A: все версии
e-STUDIO 3528AG DP-3528AG: все версии
e-STUDIO 4528A DP-4528A: все версии
e-STUDIO 4528AG DP-4528AG: все версии
e-STUDIO 5528A DP-5528A: все версии
e-STUDIO 6528A DP-6528A: все версии
e-STUDIO 6526AC FC-6526AC: все версии
e-STUDIO 6527AC FC-6527AC: все версии
e-STUDIO 7527AC FC-7527AC: все версии
e-STUDIO 6529A DP-6529A: все версии
e-STUDIO 7529A DP-7529A: все версии
e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27173

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии
e-STUDIO 2521AC FC-2521AC: все версии
e-STUDIO 2020AC FC-2020AC: все версии
e-STUDIO 2520AC FC-2520AC: все версии
e-STUDIO 2025NC FC-2025AC: все версии
e-STUDIO 2525AC FC-2525AC: все версии
e-STUDIO 3025AC FC-3025AC: все версии
e-STUDIO 3525AC FC-3525AC: все версии
e-STUDIO 3525ACG FC-3525ACG: все версии
e-STUDIO 4525AC FC-4525AC: все версии
e-STUDIO 4525ACG FC-4525ACG: все версии
e-STUDIO 5525AC FC-5525AC: все версии
e-STUDIO 5525ACG FC-5525ACG: все версии
e-STUDIO 6525AC FC-6525AC: все версии
e-STUDIO 6525ACG FC-6525ACG: все версии
e-STUDIO 2528A DP-2528A: все версии
e-STUDIO 3028A DP-3028A: все версии
e-STUDIO 3528A DP-3528A: все версии
e-STUDIO 3528AG DP-3528AG: все версии
e-STUDIO 4528A DP-4528A: все версии
e-STUDIO 4528AG DP-4528AG: все версии
e-STUDIO 5528A DP-5528A: все версии
e-STUDIO 6528A DP-6528A: все версии
e-STUDIO 6526AC FC-6526AC: все версии
e-STUDIO 6527AC FC-6527AC: все версии
e-STUDIO 7527AC FC-7527AC: все версии
e-STUDIO 6529A DP-6529A: все версии
e-STUDIO 7529A DP-7529A: все версии
e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27145

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27144

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Отказ в обслуживании в Service Interconnect 1.5

Идентификатор уязвимости: CVE-2023-45288

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: Service Interconnect: до версии 1.5.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

7

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://access.redhat.com/errata/RHSA-2024:4034>
- <https://bdu.fstec.ru/vul/2024-02688>

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27174

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27173

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27145

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27144

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Выполнение произвольного кода в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27155

Идентификатор программной ошибки: CWE-276 Некорректные разрешения, назначаемые по умолчанию

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.7 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Выполнение произвольного кода в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-3498

Идентификатор программной ошибки: CWE-250 Выполнение операций с избыточными привилегиями

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Выполнение произвольного кода в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27143

Идентификатор программной ошибки: CWE-250 Выполнение операций с избыточными привилегиями

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии
e-STUDIO 2521AC FC-2521AC: все версии
e-STUDIO 2020AC FC-2020AC: все версии
e-STUDIO 2520AC FC-2520AC: все версии
e-STUDIO 2025NC FC-2025AC: все версии
e-STUDIO 2525AC FC-2525AC: все версии
e-STUDIO 3025AC FC-3025AC: все версии
e-STUDIO 3525AC FC-3525AC: все версии
e-STUDIO 3525ACG FC-3525ACG: все версии
e-STUDIO 4525AC FC-4525AC: все версии
e-STUDIO 4525ACG FC-4525ACG: все версии
e-STUDIO 5525AC FC-5525AC: все версии
e-STUDIO 5525ACG FC-5525ACG: все версии
e-STUDIO 6525AC FC-6525AC: все версии
e-STUDIO 6525ACG FC-6525ACG: все версии
e-STUDIO 2528A DP-2528A: все версии
e-STUDIO 3028A DP-3028A: все версии
e-STUDIO 3528A DP-3528A: все версии
e-STUDIO 3528AG DP-3528AG: все версии
e-STUDIO 4528A DP-4528A: все версии
e-STUDIO 4528AG DP-4528AG: все версии
e-STUDIO 5528A DP-5528A: все версии
e-STUDIO 6528A DP-6528A: все версии
e-STUDIO 6526AC FC-6526AC: все версии
e-STUDIO 6527AC FC-6527AC: все версии
e-STUDIO 7527AC FC-7527AC: все версии
e-STUDIO 6529A DP-6529A: все версии
e-STUDIO 7529A DP-7529A: все версии
e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Чтение локальных файлов в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-3497

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Получение конфиденциальной информации в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-3496

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Выполнение произвольного кода в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27172

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии
e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии

e-STUDIO 5516AC FC-5516AC: все версии
e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии

e-STUDIO 5508A DP-5508A: все версии
e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Обход безопасности в Toshiba Tec MFPS

Идентификатор уязвимости: CVE-2024-27169

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: Toshiba Tec MFPS:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Выполнение произвольного кода в Toshiba Tec MFPs

Идентификатор уязвимости: CVE-2024-27165

Идентификатор программной ошибки: CWE-272 Нарушение принципа минимальных привилегий

Уязвимый продукт: Toshiba Tec MFPs:

e-STUDIO 2021AC FC-2021AC: все версии

e-STUDIO 2521AC FC-2521AC: все версии

e-STUDIO 2020AC FC-2020AC: все версии

e-STUDIO 2520AC FC-2520AC: все версии

e-STUDIO 2025NC FC-2025AC: все версии

e-STUDIO 2525AC FC-2525AC: все версии

e-STUDIO 3025AC FC-3025AC: все версии

e-STUDIO 3525AC FC-3525AC: все версии

e-STUDIO 3525ACG FC-3525ACG: все версии

e-STUDIO 4525AC FC-4525AC: все версии

e-STUDIO 4525ACG FC-4525ACG: все версии

e-STUDIO 5525AC FC-5525AC: все версии

e-STUDIO 5525ACG FC-5525ACG: все версии

e-STUDIO 6525AC FC-6525AC: все версии

e-STUDIO 6525ACG FC-6525ACG: все версии

e-STUDIO 2528A DP-2528A: все версии

e-STUDIO 3028A DP-3028A: все версии

e-STUDIO 3528A DP-3528A: все версии

e-STUDIO 3528AG DP-3528AG: все версии

e-STUDIO 4528A DP-4528A: все версии

e-STUDIO 4528AG DP-4528AG: все версии

e-STUDIO 5528A DP-5528A: все версии

e-STUDIO 6528A DP-6528A: все версии

e-STUDIO 6526AC FC-6526AC: все версии

e-STUDIO 6527AC FC-6527AC: все версии

e-STUDIO 7527AC FC-7527AC: все версии

e-STUDIO 6529A DP-6529A: все версии

e-STUDIO 7529A DP-7529A: все версии

e-STUDIO 9029A DP-9029A: все версии

e-STUDIO 330AC FC-330AC: все версии
e-STUDIO 400AC FC-400AC: все версии
e-STUDIO 2010AC FC-2010AC: все версии
e-STUDIO 2110AC FC-2110AC: все версии
e-STUDIO 2510AC FC-2510AC: все версии
e-STUDIO 2610AC FC-2610AC: все версии
e-STUDIO 2015NC FC-2015AC: все версии
e-STUDIO 2515AC FC-2515AC: все версии
e-STUDIO 2615AC FC-2615AC: все версии
e-STUDIO 3015AC FC-3015AC: все версии
e-STUDIO 3115AC FC-3115AC: все версии
e-STUDIO 3515AC FC-3515AC: все версии
e-STUDIO 3615AC FC-3615AC: все версии
e-STUDIO 4515AC FC-4515AC: все версии
e-STUDIO 4615AC FC-4615AC: все версии
e-STUDIO 5015AC FC-5015AC: все версии
e-STUDIO 5115AC FC-5115AC: все версии
e-STUDIO 2018A DP-2018A: все версии
e-STUDIO 2518A DP-2518A: все версии
e-STUDIO 2618A DP-2618A: все версии
e-STUDIO 3018A DP-3018A: все версии
e-STUDIO 3118A DP-3118A: все версии
e-STUDIO 3018AG DP-3018AG: все версии
e-STUDIO 3518A DP-3518A: все версии
e-STUDIO 3518AG DP-3518AG: все версии
e-STUDIO 3618A DP-3618A: все версии
e-STUDIO 3618AG DP-3618AG: все версии
e-STUDIO 4518A DP-4518A: все версии
e-STUDIO 4518AG DP-4518AG: все версии
e-STUDIO 4618A DP-4618A: все версии
e-STUDIO 4618AG DP-4618AG: все версии
e-STUDIO 5018A DP-5018A: все версии
e-STUDIO 5118A DP-5118A: все версии
e-STUDIO 5516AC FC-5516AC: все версии

e-STUDIO 5616AC FC-5616AC: все версии
e-STUDIO 6516AC FC-6516AC: все версии
e-STUDIO 6616AC FC-6616AC: все версии
e-STUDIO 7516AC FC-7516AC: все версии
e-STUDIO 7616AC FC-7616AC: все версии
e-STUDIO 5518A DP-5518A: все версии
e-STUDIO 5618A DP-5618A: все версии
e-STUDIO 6518A DP-6518A: все версии
e-STUDIO 6618A DP-6618A: все версии
e-STUDIO 7518A DP-7518A: все версии
e-STUDIO 7618A DP-7618A: все версии
e-STUDIO 8518A DP-8518A: все версии
e-STUDIO 8618A DP-8618A: все версии
e-STUDIO 2000AC FC-2000AC: все версии
e-STUDIO 2500AC FC-2500AC: все версии
e-STUDIO 2005NC FC-2005AC: все версии
e-STUDIO 2505AC FC-2005AC: все версии
e-STUDIO 3005AC FC-2005AC: все версии
e-STUDIO 3505AC FC-2005AC: все версии
e-STUDIO 4505AC FC-2005AC: все версии
e-STUDIO 5005AC FC-2005AC: все версии
e-STUDIO 2008A DP-2008A: все версии
e-STUDIO 2508A DP-2508A: все версии
e-STUDIO 3008A DP-3008A: все версии
e-STUDIO 3008AG DP-3008AG: все версии
e-STUDIO 3508A DP-3508A: все версии
e-STUDIO 3508AG DP-3508AG: все версии
e-STUDIO 4508A DP-4508A: все версии
e-STUDIO 4508AG DP-4508AG: все версии
e-STUDIO 5008A DP-5008A: все версии
e-STUDIO 5506AC FC-5506AC: все версии
e-STUDIO 6506AC FC-6506AC: все версии
e-STUDIO 7506AC FC-7506AC: все версии
e-STUDIO 5508A DP-5508A: все версии

e-STUDIO 6508A DP-6508A: все версии
e-STUDIO 7508A DP-7508A: все версии
e-STUDIO 8508A DP-8508A: все версии
e-STUDIO 3508LP DP-3535: все версии
e-STUDIO 4508LP DP-4535: все версии
e-STUDIO 5008LP DP-5035: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-20 / 2024-06-20

Ссылки на источник:

- <http://jvn.jp/en/vu/JVNVU97136265/index.html>
- http://www.toshibatec.com/information/20240531_01.html

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-6103

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 126.0.2592.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

20 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-6103>

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-6101

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 126.0.2592.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

21 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-6101>

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-6102

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 126.0.2592.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

22 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-6102>

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-6100

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 по 126.0.2592.61

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

23 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-21 / 2024-06-21

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-6100>

Краткое описание: Повышение привилегий в VMware vCenter Server

Идентификатор уязвимости: CVE-2024-37081

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: vCenter Server: с версии 7.0 U1 по 8.0.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

24 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- <http://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453>

Краткое описание: Выполнение произвольного кода в VMware vCenter Server

Идентификатор уязвимости: CVE-2024-37080

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: vCenter Server: с версии 7.0 U1 по 8.0.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

25

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- <http://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453>
- <https://bdu.fstec.ru/vul/2024-04780>

26

Краткое описание: Выполнение произвольного кода в VMware vCenter Server

Идентификатор уязвимости: CVE-2024-37079

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: vCenter Server: с версии 7.0 U1 по 8.0.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- <http://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453>
- <https://bdu.fstec.ru/vul/2024-04649>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-36999

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

27 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-789/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23159

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

28 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-794/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23158

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

29 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-798/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23157

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

30

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:HI/H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-800/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-685/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23156

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

31

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевое экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:HI/H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-799/>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-796/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23155

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

32 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-787/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23154

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

33 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-790/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23151

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

34 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-793/>

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-23150

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk AutoCAD: с версии 2024 по 2024.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

35 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-19 / 2024-06-19

Ссылки на источник:

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-792/>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6103

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 126.0.6478.62

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

36

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_18.html
- <http://crbug.com/344639860>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6102

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 126.0.6478.62

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

37

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_18.html
- <http://crbug.com/339169163>

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-6101

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 126.0.6478.62

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

38

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_18.html
- <http://crbug.com/343748812>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6100

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смещение типов)

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 126.0.6478.62

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

39

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_18.html
- <http://crbug.com/344608204>

Краткое описание: Выполнение произвольного кода в Dropbox Desktop

Идентификатор уязвимости: CVE-2024-5924

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Dropbox Desktop: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

40 Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевое экранирования или другими административными мерами.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-677/>

Краткое описание: Выполнение произвольного кода в Gnome gdk-pixbuf

Идентификатор уязвимости: CVE-2022-48622

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Gnome gdk-pixbuf: с версии 2.42.0 по 2.42.10

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

41

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-18 / 2024-06-18

Ссылки на источник:

- <http://gitlab.gnome.org/GNOME/gdk-pixbuf/-/issues/202>