НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-09-16.1 | 16 сентября 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-8232	SpiderControl SCADA Web Server	Сетевой	WLF	2024-09-13	✓
2	Высокая	CVE-2024-45823	Rockwell Automation FactoryTalk Batch View	Сетевой	SB	2024-09-13	✓
3	Критическая	CVE-2024-45824	Rockwell Automation FactoryTalk View Site	Сетевой	ACE	2024-09-13	✓
4	Критическая	CVE-2024-38476	F5 Traffix SDC Apache HTTPD component	Сетевой	CSRF	2024-09-13	✗
5	Высокая	CVE-2024-20381	multiple Cisco products	Сетевой	SB	2024-09-13	✓
6	Высокая	CVE-2024-20304	Cisco IOS XR software	Сетевой	DoS	2024-09-12	✓
7	Критическая	CVE-2024-30949	newlib	Сетевой	ACE	2024-09-12	✓
8	Критическая	CVE-2024-22399	Apache Seata	Сетевой	ACE	2024-09-12	✓
9	Критическая	CVE-2024-8362	Microsoft Edge	Сетевой	ACE	2024-09-12	✓
10	Критическая	CVE-2024-7970	Microsoft Edge	Сетевой	ACE	2024-09-12	✓
11	Высокая	CVE-2024-8194	Microsoft Edge	Сетевой	ACE	2024-09-12	✓
12	Высокая	CVE-2024-8198	Microsoft Edge	Сетевой	ACE	2024-09-12	✓
13	Критическая	CVE-2024-45492	Nessus Agent	Сетевой	ACE	2024-09-11	✓

14	Критическая	CVE-2024-45491	Nessus Agent	Сетевой	ACE	2024-09-11	✓
15	Высокая	CVE-2024-6119	Nessus Agent	Сетевой	DoS	2024-09-11	✓
16	Критическая	CVE-2024-33698	Siemens User Management Component (UMC)	Сетевой	ACE	2024-09-11	✓
17	Высокая	CVE-2024-41170	Siemens Tecnomatix Plant Simulation	Локальный	ACE	2024-09-11	✓
18	Критическая	CVE-2024-45032	Siemens Industrial Edge Management	Сетевой	SB	2024-09-11	✓
19	Высокая	CVE-2024-44087	Siemens Automation License Manager	Сетевой	DoS	2024-09-11	✓
20	Критическая	CVE-2024-29847	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
21	Высокая	CVE-2024-8191	Ivanti Endpoint Manager	Локальный	ACE	2024-09-11	✓
22	Критическая	CVE-2024-32840	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
23	Критическая	CVE-2024-32842	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
24	Критическая	CVE-2024-32843	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
25	Критическая	CVE-2024-32845	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
26	Критическая	CVE-2024-32846	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
27	Критическая	CVE-2024-32848	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
28	Высокая	CVE-2024-37397	Ivanti Endpoint Manager	Сетевой	OSI	2024-09-11	✓

29	Критическая	CVE-2024-34779	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
30	Критическая	CVE-2024-34785	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
31	Критическая	CVE-2024-34783	Ivanti Endpoint Manager	Сетевой	ACE	2024-09-11	✓
32	Высокая	CVE-2024-8639	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-11	✓
33	Высокая	CVE-2024-8638	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-11	✓
34	Высокая	CVE-2024-8637	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-11	✓
35	Высокая	CVE-2024-8636	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-09-11	✓
36	Высокая	CVE-2024-38240	Microsoft Windows Remote Access Connection Manager	Сетевой	PE	2024-09-10	✓
37	Высокая	CVE-2024-43465	Microsoft Excel	Локальный	PE	2024-09-10	✓
38	Высокая	CVE-2024-39384	Adobe Premiere Pro	Локальный	ACE	2024-09-10	✓
39	Критическая	CVE-2024-41874	Adobe ColdFusion	Сетевой	ACE	2024-09-10	✓
40	Высокая	CVE-2024-39378	Adobe Audition	Локальный	ACE	2024-09-10	✓
41	Высокая	CVE-2024-45109	Adobe Photoshop	Локальный	ACE	2024-09-10	✓
42	Высокая	CVE-2024-45108	Adobe Photoshop	Локальный	ACE	2024-09-10	✓
43	Высокая	CVE-2024-43760	Adobe Photoshop	Локальный	ACE	2024-09-10	✓

44	Высокая	CVE-2024-43756	Adobe Photoshop	Локальный	ACE	2024-09-10	✓
45	Высокая	CVE-2024-39377	Adobe Media Encoder	Локальный	ACE	2024-09-10	✓
46	Высокая	CVE-2024-41856	Adobe Illustrator	Локальный	ACE	2024-09-10	✓
47	Высокая	CVE-2024-43758	Adobe Illustrator	Локальный	ACE	2024-09-10	✓
48	Высокая	CVE-2024-34121	Adobe Illustrator	Локальный	ACE	2024-09-10	✓
49	Высокая	CVE-2024-41857	Adobe Illustrator	Локальный	ACE	2024-09-10	✓
50	Высокая	CVE-2024-41859	Adobe After Effects	Локальный	ACE	2024-09-10	✓
51	Высокая	CVE-2024-39381	Adobe After Effects	Локальный	ACE	2024-09-10	✓
52	Высокая	CVE-2024-39380	Adobe After Effects	Локальный	ACE	2024-09-10	✓
53	Высокая	CVE-2024-43463	Microsoft Office Visio	Локальный	ACE	2024-09-10	✓
54	Высокая	CVE-2024-45112	Adobe Acrobat and Reader	Локальный	ACE	2024-09-10	✓
55	Высокая	CVE-2024-41869	Adobe Acrobat and Reader	Локальный	ACE	2024-09-10	✓
56	Высокая	CVE-2024-38259	Microsoft Management Console	Сетевой	ACE	2024-09-10	✓
57	Высокая	CVE-2024-43461	Microsoft Windows MSHTML Platform and Internet Explorer	Сетевой	OSI	2024-09-10	✓
58	Высокая	CVE-2024-21416	Microsoft Windows NetNAT service	Сетевой	ACE	2024-09-10	✓

59	Высокая	CVE-2024-38045	Microsoft Windows NetNAT service	Сетевой	ACE	2024-09-10	✓
60	Высокая	CVE-2024-38226	Microsoft Publisher	Сетевой	ACE	2024-09-10	✓
61	Высокая	CVE-2024-38014	Microsoft Windows Installer	Локальный	ACE	2024-09-10	✓
62	Критическая	CVE-2024-43491	Microsoft Windows Update	Сетевой	ACE	2024-09-10	✓
63	Высокая	CVE-2024-40896	Libxml2	Сетевой	OSI	2024-09-10	✓
64	Высокая	CVE-2024-32228	FFmpeg	Сетевой	ACE	2024-09-10	✓
65	Высокая	CVE-2024-7974	Google ChromeOS	Сетевой	OSI	2024-09-10	✓
66	Высокая	CVE-2024-7972	Google ChromeOS	Сетевой	OSI	2024-09-10	✓
67	Высокая	CVE-2024-7971	Google ChromeOS	Сетевой	ACE	2024-09-10	✓
68	Высокая	CVE-2024-7968	Google ChromeOS	Сетевой	ACE	2024-09-10	✓
69	Высокая	CVE-2024-7967	Google ChromeOS	Сетевой	ACE	2024-09-10	✓
70	Высокая	CVE-2024-7966	Google ChromeOS	Сетевой	ACE	2024-09-10	✓
71	Высокая	CVE-2024-7965	Google ChromeOS	Сетевой	OSI	2024-09-10	✓
72	Критическая	CVE-2024-7591	Progress LoadMaster	Сетевой	ACE	2024-09-09	✓

1

Краткое описание: Запись локальных файлов в SpiderControl SCADA Web Server

Идентификатор уязвимости: CVE-2024-8232

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: SCADAWebServer: 2.09

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись 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:N/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-13 / 2024-09-13

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-254-02

2

Краткое описание: Обход безопасности в Rockwell Automation FactoryTalk Batch View

Идентификатор уязвимости: CVE-2024-45823

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: FactoryTalk Batch View: 2.01.00

Категория уязвимого продукта: Прикладное программное обеспечение

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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-13 / 2024-09-13

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD%201698.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-256-22

Краткое описание: Выполнение произвольного кода в Rockwell Automation FactoryTalk View Site

Идентификатор уязвимости: CVE-2024-45824
BDU:2024-06876

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: FactoryTalk View Site Edition: 12.0 - 14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

3 **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: 2024-09-13 / 2024-09-13

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1696.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-256-23
- https://bdu.fstec.ru/vul/2024-06876

4

Краткое описание: Подделка запросов на стороне сервера в F5 Traffix SDC Apache HTTPD component

Идентификатор уязвимости: CVE-2024-38476
BDU:2024-05131

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: Traffix SDC: 5.1.0 - 5.2.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Подделка запросов на стороне сервера

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

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: 2024-09-13 / 2024-09-13

Ссылки на источник:

- http://my.f5.com/manage/s/article/K000140618
- https://bdu.fstec.ru/vul/2024-05131

Краткое описание: Обход безопасности в multiple Cisco products

Идентификатор уязвимости: CVE-2024-20381

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Crosswork Network Services Orchestrator: 5.5 - 6.2
Optical Site Manager: 24.3
Cisco RV340 Dual WAN Gigabit VPN Router: все версии
ConfD: 7.5 - 8.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

5 **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: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-13 / 2024-09-13

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-auth-bypass-QnTEesp

6

Краткое описание: Отказ в обслуживании в Cisco IOS XR software

Идентификатор уязвимости: CVE-2024-20304
BDU:2024-06877

Идентификатор программной ошибки: CWE-401 Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)

Уязвимый продукт: Cisco IOS XR: 7.7.0 - 24.2.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pak-mem-exhst-3ke9FeFy
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwk63828
- https://bdu.fstec.ru/vul/2024-06877

7

Краткое описание: Выполнение произвольного кода в newlib

Идентификатор уязвимости: CVE-2024-30949

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: newlib: 3.0.0 - 4.3.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://inbox.sourceware.org/newlib/20231129035714.469943-1-visitorckw%40gmail.com/
- http://sourceware.org/git/?p=newlib-cygwin.git%3Ba=commit%3Bh=5f15d7c5817b07a6b18cbab17342c95cb7b42be4
- http://gist.github.com/visitorckw/6b26e599241ea80210ea136b28441661

8

Краткое описание: Выполнение произвольного кода в Apache Seata

Идентификатор уязвимости: CVE-2024-22399

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Apache Seata: 1.0.0 - 2.0.0

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:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://lists.apache.org/thread/kdzzbn3vt1qt4r6jgqbswphkh6b9jwyw

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-8362

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 128.0.2739.54

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

9 **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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-8362

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7970

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 128.0.2739.54

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

10 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-7970

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-8194
BDU:2024-06723

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 128.0.2739.42

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

11 **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: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-8194
- https://bdu.fstec.ru/vul/2024-06723

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-8198
BDU:2024-06725

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 128.0.2739.42

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

12 **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: 2024-09-12 / 2024-09-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-8198
- https://bdu.fstec.ru/vul/2024-06725

13

Краткое описание: Выполнение произвольного кода в Nessus Agent

Идентификатор уязвимости: CVE-2024-45492

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Nessus Agent: 10.0.0 - 10.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-14

14

Краткое описание: Выполнение произвольного кода в Nessus Agent

Идентификатор уязвимости: CVE-2024-45491

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Nessus Agent: 10.0.0 - 10.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-14

Краткое описание: Отказ в обслуживании в Nessus Agent

Идентификатор уязвимости: CVE-2024-6119
BDU:2024-06735

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

Уязвимый продукт: Nessus Agent: 10.0.0 - 10.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

15 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-14
- https://bdu.fstec.ru/vul/2024-06735

16

Краткое описание: Выполнение произвольного кода в Siemens User Management Component (UMC)

Идентификатор уязвимости: CVE-2024-33698

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

Уязвимый продукт: SIMATIC Information Server: 2022 - 2024
SIMATIC PCS neo: 4.0 - 5.0
SINEC NMS: все версии
Totally Integrated Automation Portal (TIA Portal): 16 - 19

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-039007.html
- http://www.tenable.com/security/research/tra-2024-37-0

Краткое описание: Выполнение произвольного кода в Siemens Tecnomatix Plant Simulation

Идентификатор уязвимости: CVE-2024-41170
BDU:2024-06829

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tecnomatix Plant Simulation: 2302 - 2404

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

17 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-427715.html
- https://bdu.fstec.ru/vul/2024-06829

Краткое описание: Обход безопасности в Siemens Industrial Edge Management

Идентификатор уязвимости: CVE-2024-45032

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: Industrial Edge Management Pro: до 1.9.5
Industrial Edge Management Virtual: до 2.3.1-1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

18

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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-359713.html

19

Краткое описание: Отказ в обслуживании в Siemens Automation License Manager

Идентификатор уязвимости: CVE-2024-44087

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Siemens Automation License Manager: 5.0 - 6.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-103653.html

20

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-29847
BDU:2024-06794

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1223/
- https://bdu.fstec.ru/vul/2024-06794

21

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-8191

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированного запроса.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1211/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-32840

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1213/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-32842

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1214/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-32843

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1215/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-32845

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1216/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-32846

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

26 **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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1217/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-32848

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

27 **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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1218/

28

Краткое описание: Получение конфиденциальной информации в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-37397

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

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: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1212/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-34779

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

29 **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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1219/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-34785

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

30 **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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1221/

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2024-34783

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Endpoint Manager: 2022 - 2024 July Update

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

31 **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: 9.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- http://www.zerodayinitiative.com/advisories/ZDI-24-1220/

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-8639

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.120
Microsoft Edge: 100.0.1185.29 - 128.0.2739.67

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

32 **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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html
- http://crbug.com/362658609
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-8639

33

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-8638

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.120
Microsoft Edge: 100.0.1185.29 - 128.0.2739.67

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html
- http://crbug.com/362539773
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-8638

34

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-8637

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.120
Microsoft Edge: 100.0.1185.29 - 128.0.2739.67

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html
- http://crbug.com/361784548
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-8637

35

Краткое описание: Выполнение произвольного кода в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-8636

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 128.0.6613.120
Microsoft Edge: 100.0.1185.29 - 128.0.2739.67

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-09-11 / 2024-09-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_10.html
- http://crbug.com/361461526
- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-8636

Краткое описание: Повышение привилегий в Microsoft Windows Remote Access Connection Manager

Идентификатор уязвимости: CVE-2024-38240

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows: до 11 24H2 10.0.26100.1742
Windows Server: до 2022 23H2 10.0.25398.1128

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38240

Краткое описание: Повышение привилегий в Microsoft Excel

Идентификатор уязвимости: CVE-2024-43465

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Office Online Server : все версии
Microsoft Excel: 2016
Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

37

Последствия эксплуатации: Повышение привилегий

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43465

38

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2024-39384

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Premiere Pro: 22.0 - 24.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/premiere_pro/apsb24-58.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1201/

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2024-41874

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: ColdFusion: 2016 - 2023 Update 9

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb24-71.html

40

Краткое описание: Выполнение произвольного кода в Adobe Audition

Идентификатор уязвимости: CVE-2024-39378

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Audition: 22.0 - 24.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/audition/apsb24-54.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1197/

41

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-45109

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Photoshop: 20.0 - 25.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb24-72.html

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-45108

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Photoshop: 20.0 - 25.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

42 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb24-72.html

43

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-43760

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Photoshop: 20.0 - 25.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb24-72.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1203/

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-43756

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

Уязвимый продукт: Adobe Photoshop: 20.0 - 25.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

44 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb24-72.html

45

Краткое описание: Выполнение произвольного кода в Adobe Media Encoder

Идентификатор уязвимости: CVE-2024-39377

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Media Encoder: 22.0 - 24.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/media-encoder/apsb24-53.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1200/

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-41856

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

46 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb24-66.html

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-43758

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

47 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb24-45.html

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-34121

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

48 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb24-66.html

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-41857

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

49 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb24-66.html

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2024-41859

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 24.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

50 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb24-55.html

51

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2024-39381

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: 22.0 - 24.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb24-55.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1202/

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2024-39380

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

Уязвимый продукт: Adobe After Effects: 22.0 - 24.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

52 **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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb24-55.html

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2024-43463

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Microsoft Visio: 2016
Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

53 **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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43463

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-45112

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

Уязвимый продукт: Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.003.20054

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

54

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-70.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-41869

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.003.20054

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

55

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-70.html

Краткое описание: Выполнение произвольного кода в Microsoft Management Console

Идентификатор уязвимости: CVE-2024-38259

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server: до 2022 23H2 10.0.25398.1128
Windows: до 11 24H2 10.0.26100.1742

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

56

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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38259

Краткое описание: Получение конфиденциальной информации в Microsoft Windows MSHTML Platform and Internet Explorer

Идентификатор уязвимости: CVE-2024-43461

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Microsoft Internet Explorer: 11 - 11.1790.17763.0
Windows: до 11 24H2 10.0.26100.1742
Windows Server: до 2022 23H2 10.0.25398.1128

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

57 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43461
- http://www.zerodayinitiative.com/blog/2024/9/10/the-september-2024-security-update-review
- http://www.zerodayinitiative.com/advisories/ZDI-24-1207/

Краткое описание: Выполнение произвольного кода в Microsoft Windows NetNAT service

Идентификатор уязвимости: CVE-2024-21416

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

Уязвимый продукт: Windows: до 11 24H2 10.0.26100.1742
Windows Server: до 2022 23H2 10.0.25398.1128

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

58

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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-21416

Краткое описание: Выполнение произвольного кода в Microsoft Windows NetNAT service

Идентификатор уязвимости: CVE-2024-38045

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

Уязвимый продукт: Windows: до 11 24H2 10.0.26100.1742
Windows Server: до 2022 23H2 10.0.25398.1128

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

59

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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38045

Краткое описание: Выполнение произвольного кода в Microsoft Publisher

Идентификатор уязвимости: CVE-2024-38226
BDU:2024-06873

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Microsoft Office: 2016 - 2019
Microsoft Publisher: до 16.0.5465.1001

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

60

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: 8.0 AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38226
- https://bdu.fstec.ru/vul/2024-06873

Краткое описание: Выполнение произвольного кода в Microsoft Windows Installer

Идентификатор уязвимости: CVE-2024-38014
BDU:2024-06875

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Windows: до 11 24H2 10.0.26100.1742
Windows Server: до 2022 23H2 10.0.25398.1128

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

61

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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38014
- https://bdu.fstec.ru/vul/2024-06875

Краткое описание: Выполнение произвольного кода в Microsoft Windows Update

Идентификатор уязвимости: CVE-2024-43491
BDU:2024-06872

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 11 24H2 10.0.26100.1742

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

62 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43491
- https://bdu.fstec.ru/vul/2024-06872

Краткое описание: Получение конфиденциальной информации в Libxml2

Идентификатор уязвимости: CVE-2024-40896

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Libxml2: 2.11.0 - 2.13.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Получение конфиденциальной информации

63 **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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://gitlab.gnome.org/GNOME/libxml2/-/issues/761

64

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2024-32228

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

Уязвимый продукт: FFmpeg: 6.0 - 7.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10951

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7974

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

65 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7972
BDU:2024-06711

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

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

66 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html
- https://bdu.fstec.ru/vul/2024-06711

67

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7971
BDU:2024-06562

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

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

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

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: 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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html
- https://bdu.fstec.ru/vul/2024-06562

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7968
BDU:2024-06585

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

68 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html
- https://bdu.fstec.ru/vul/2024-06585

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7967
BDU:2024-06553

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

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

69 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html
- https://bdu.fstec.ru/vul/2024-06553

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7966
BDU:2024-06567

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

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

70 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html
- https://bdu.fstec.ru/vul/2024-06567

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2024-7965

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

Уязвимый продукт: Chrome OS: до 128.0.6613.133

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

71 **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: 2024-09-10 / 2024-09-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-chromeos_9.html

72

Краткое описание: Выполнение произвольного кода в Progress LoadMaster

Идентификатор уязвимости: CVE-2024-7591

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

Уязвимый продукт: LoadMaster: до 7.2.60.0.22520
Multi-Tenant Hypervisor: до 7.2.60.0.22520

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-09-09 / 2024-09-09

Ссылки на источник:

- http://support.kemptechnologies.com/hc/en-us/articles/29196371689613-LoadMaster-Security-Vulnerability-CVE-2024-7591