НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-08-28.1 | 28 августа 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-38653	Ivanti Avalanche	Сетевой	OSI	2024-08-14	✓
2	Высокая	CVE-2024-36136	Ivanti Avalanche	Сетевой	DoS	2024-08-14	✓
3	Высокая	CVE-2024-37399	Ivanti Avalanche	Сетевой	DoS	2024-08-14	✓
4	Высокая	CVE-2024-38652	Ivanti Avalanche	Сетевой	RLF	2024-08-14	✓
5	Высокая	CVE-2024-7570	Ivanti Neurons for ITSM	Сетевой	OSI	2024-08-14	✓
6	Критическая	CVE-2024-7569	Ivanti Neurons for ITSM	Сетевой	OSI	2024-08-14	✓
7	Высокая	CVE-2024-38116	Microsoft Windows IP Routing Management Snapin	Сетевой	ACE	2024-08-13	✓
8	Высокая	CVE-2024-38114	Microsoft Windows IP Routing Management Snapin	Сетевой	ACE	2024-08-13	✓
9	Высокая	CVE-2024-38115	Microsoft Windows IP Routing Management Snapin	Сетевой	ACE	2024-08-13	✓
10	Высокая	CVE-2024-38177	Microsoft Windows App Installer	Локальный	OSI	2024-08-14	✓
11	Высокая	CVE-2024-38152	Microsoft Windows OLE	Локальный	ACE	2024-08-13	✓
12	Высокая	CVE-2024-41851	Adobe InDesign	Локальный	ACE	2024-08-13	✓
13	Высокая	CVE-2024-41850	Adobe InDesign	Локальный	ACE	2024-08-13	✓

14	Высокая	CVE-2024-39394	Adobe InDesign	Локальный	ACE	2024-08-13	✓
15	Высокая	CVE-2024-39393	Adobe InDesign	Локальный	OSI	2024-08-13	✓
16	Высокая	CVE-2024-41853	Adobe InDesign	Локальный	ACE	2024-08-13	✓
17	Высокая	CVE-2024-41852	Adobe InDesign	Локальный	ACE	2024-08-13	✓
18	Высокая	CVE-2024-39391	Adobe InDesign	Локальный	ACE	2024-08-13	✓
19	Высокая	CVE-2024-39390	Adobe InDesign	Локальный	ACE	2024-08-13	✓
20	Высокая	CVE-2024-39389	Adobe InDesign	Локальный	ACE	2024-08-13	✓
21	Высокая	CVE-2024-38169	Microsoft Office Visio	Локальный	ACE	2024-08-14	✓
22	Критическая	CVE-2024-38140	Microsoft Windows Reliable Multicast Transport Driver (RMCAST)	Сетевой	ACE	2024-08-14	✓
23	Высокая	CVE-2024-34133	Adobe Illustrator	Локальный	ACE	2024-08-13	✓
24	Высокая	CVE-2024-29995	Microsoft Windows Kerberos	Сетевой	PE	2024-08-13	✓
25	Высокая	CVE-2024-20789	Adobe Dimension	Локальный	ACE	2024-08-13	✓
26	Высокая	CVE-2024-41865	Adobe Dimension	Локальный	ACE	2024-08-13	✓
27	Высокая	CVE-2024-34124	Adobe Dimension	Локальный	ACE	2024-08-13	✓
28	Высокая	CVE-2024-41840	Adobe Bridge	Локальный	ACE	2024-08-13	✓

29	Высокая	CVE-2024-39386	Adobe Bridge	Локальный	ACE	2024-08-13	✓
30	Высокая	CVE-2024-38180	Microsoft Windows SmartScreen	Сетевой	SB	2024-08-14	✓
31	Высокая	CVE-2024-38170	Microsoft Excel	Сетевой	ACE	2024-08-14	✓
32	Высокая	CVE-2024-38172	Microsoft Excel	Сетевой	ACE	2024-08-14	✓
33	Высокая	CVE-2024-41831	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
34	Высокая	CVE-2024-41830	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
35	Высокая	CVE-2024-39426	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
36	Высокая	CVE-2024-39425	Adobe Acrobat and Reader	Локальный	PE	2024-08-13	✓
37	Высокая	CVE-2024-39424	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
38	Высокая	CVE-2024-39423	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
39	Высокая	CVE-2024-39422	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
40	Высокая	CVE-2024-39383	Adobe Acrobat and Reader	Локальный	ACE	2024-08-13	✓
41	Высокая	CVE-2024-39399	Adobe Commerce and Magento Open Source	Сетевой	RLF	2024-08-14	✓
42	Высокая	CVE-2024-39400	Adobe Commerce and Magento Open Source	Сетевой	XSS\CSS	2024-08-14	✓

43	Высокая	CVE-2024-39401	Adobe Commerce and Magento Open Source	Сетевой	ACE	2024-08-14	✓
44	Высокая	CVE-2024-39402	Adobe Commerce and Magento Open Source	Сетевой	ACE	2024-08-14	✓
45	Высокая	CVE-2024-39403	Adobe Commerce and Magento Open Source	Сетевой	XSS\CSS	2024-08-14	✓
46	Критическая	CVE-2024-39397	Adobe Commerce and Magento Open Source	Сетевой	WLF	2024-08-14	✓
47	Критическая	CVE-2024-38199	Microsoft Windows Line Printer Daemon (LPD) Service	Сетевой	ACE	2024-08-13	✓
48	Высокая	CVE-2024-39825	Zoom Workplace Apps and Rooms clients	Сетевой	ACE	2024-08-13	✓
49	Высокая	CVE-2024-38131	Microsoft Clipboard Virtual Channel Extension	Сетевой	ACE	2024-08-13	✓
50	Критическая	CVE-2024-38063	Microsoft Windows TCP/IP	Сетевой	ACE	2024-08-13	✓
51	Высокая	CVE-2024-38189	Microsoft Project	Сетевой	ACE	2024-08-13	✓
52	Высокая	CVE-2024-38107	Microsoft Windows Power Dependency Coordinator	Локальный	ACE	2024-08-13	✓
53	Высокая	CVE-2024-38154	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-08-13	✓
54	Высокая	CVE-2024-38121	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-08-13	✓

55	Высокая	CVE-2024-38128	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-08-13	✓
56	Высокая	CVE-2024-38120	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-08-13	✓
57	Высокая	CVE-2024-38130	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-08-13	✓
58	Высокая	CVE-2024-38106	Microsoft Windows kernel	Локальный	PE	2024-08-13	✓
59	Высокая	CVE-2024-38178	Microsoft Windows Scripting Engine	Сетевой	ACE	2024-08-13	✓
60	Высокая	CVE-2024-40898	Tenable Security Center	Сетевой	CSRF	2024-08-13	✓
61	Высокая	CVE-2024-38477	Tenable Security Center	Сетевой	DoS	2024-08-13	✓
62	Критическая	CVE-2024-38476	Tenable Security Center	Сетевой	CSRF	2024-08-13	✓
63	Высокая	CVE-2024-38475	Tenable Security Center	Сетевой	ACE	2024-08-13	✓
64	Высокая	CVE-2024-36387	Tenable Security Center	Сетевой	DoS	2024-08-13	✓
65	Критическая	CVE-2024-41730	SAP BusinessObjects Business Intelligence Platform	Сетевой	SB	2024-08-13	✓
66	Критическая	CVE-2023-49583	SAP libraries	Сетевой	OSI	2024-08-13	✓
67	Критическая	CVE-2023-50422	SAP libraries	Сетевой	OSI	2024-08-13	✓
68	Критическая	CVE-2023-50423	SAP libraries	Сетевой	OSI	2024-08-13	✓

69	Критическая	CVE-2023-50424	SAP libraries	Сетевой	OSI	2024-08-13	✓
70	Высокая	CVE-2024-35161	Apache Traffic Server	Сетевой	OSI	2024-08-12	✓
71	Высокая	CVE-2023-38522	Apache Traffic Server	Сетевой	OSI	2024-08-12	✓
72	Высокая	CVE-2024-7502	Delta Electronics DIAScreen	Локальный	ACE	2024-08-12	✓
73	Высокая	CVE-2024-43044	Jenkins and Jenkins LTS	Сетевой	ACE	2024-08-12	✓

1

Краткое описание: Получение конфиденциальной информации в Ivanti Avalanche

Идентификатор уязвимости: CVE-2024-38653

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

Уязвимый продукт: Avalanche: 6.3.1 - 6.4.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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:N/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373
- http://www.zerodayinitiative.com/advisories/ZDI-24-1150/

2

Краткое описание: Отказ в обслуживании в Ivanti Avalanche

Идентификатор уязвимости: CVE-2024-36136

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Avalanche: 6.3.1 - 6.4.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373

3

Краткое описание: Отказ в обслуживании в Ivanti Avalanche

Идентификатор уязвимости: CVE-2024-37399

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Avalanche: 6.3.1 - 6.4.3

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: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373
- http://www.zerodayinitiative.com/advisories/ZDI-24-1151/

4

Краткое описание: Чтение локальных файлов в Ivanti Avalanche

Идентификатор уязвимости: CVE-2024-38652

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

Уязвимый продукт: Avalanche: 6.3.1 - 6.4.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373
- http://www.zerodayinitiative.com/advisories/ZDI-24-1149/

5

Краткое описание: Получение конфиденциальной информации в Ivanti Neurons for ITSM

Идентификатор уязвимости: CVE-2024-7570

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Ivanti Neurons for ITSM: 2023.2 - 2023.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка сертификатов.

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2024-7569-CVE-2024-7570

6

Краткое описание: Получение конфиденциальной информации в Ivanti Neurons for ITSM

Идентификатор уязвимости: CVE-2024-7569

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: Ivanti Neurons for ITSM: 2023.2 - 2023.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2024-7569-CVE-2024-7570

Краткое описание: Выполнение произвольного кода в Microsoft Windows IP Routing Management Snapin

Идентификатор уязвимости: CVE-2024-38116
BDU:2024-06354

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38116
- https://bdu.fstec.ru/vul/2024-06354

Краткое описание: Выполнение произвольного кода в Microsoft Windows IP Routing Management Snapin

Идентификатор уязвимости: CVE-2024-38114
BDU:2024-06356

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

8

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38114
- https://bdu.fstec.ru/vul/2024-06356

Краткое описание: Выполнение произвольного кода в Microsoft Windows IP Routing Management Snapin

Идентификатор уязвимости: CVE-2024-38115
BDU:2024-06355

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38115
- https://bdu.fstec.ru/vul/2024-06355

10

Краткое описание: Получение конфиденциальной информации в Microsoft Windows App Installer

Идентификатор уязвимости: CVE-2024-38177

Идентификатор программной ошибки: CWE-116 Некорректная кодировка или очистка выходных данных

Уязвимый продукт: App Installer: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38177

Краткое описание: Выполнение произвольного кода в Microsoft Windows OLE

Идентификатор уязвимости: CVE-2024-38152

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38152

12

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-41851

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

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

13

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-41850

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

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

14

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-39394

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

15

Краткое описание: Получение конфиденциальной информации в Adobe InDesign

Идентификатор уязвимости: CVE-2024-39393

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

16

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-41853

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

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

17

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-41852

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

18

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-39391

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

19

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-39390

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-39389

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe InDesign: 11.3.0 - 19.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/indesign/apsb24-56.html

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2024-38169

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

Уязвимый продукт: Microsoft Office: 2019
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.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38169
- http://www.zerodayinitiative.com/advisories/ZDI-24-1145/

Краткое описание: Выполнение произвольного кода в Microsoft Windows Reliable Multicast Transport Driver (RMCAST)

Идентификатор уязвимости: CVE-2024-38140

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Отправка специально сформированных данных.

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: 9.8 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-34133

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

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

24

Краткое описание: Повышение привилегий в Microsoft Windows Kerberos

Идентификатор уязвимости: CVE-2024-29995
BDU:2024-06328

Идентификатор программной ошибки: CWE-208 Разглашение информации, связанное с временной разницей при выполнении операций

Уязвимый продукт: Windows: до 10 1809 10.0.17763.6189
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Не определено

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-29995
- https://bdu.fstec.ru/vul/2024-06328

25

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2024-20789

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Dimension: 3.1 - 3.4.11

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/dimension/apsb24-47.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1142/

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2024-41865

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Adobe Dimension: 3.1 - 3.4.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/dimension/apsb24-47.html

27

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2024-34124

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Dimension: 3.1 - 3.4.11

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/dimension/apsb24-47.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1143/

28

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2024-41840

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Bridge: 13.0 - 14.1.1

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/bridge/apsb24-59.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1138/

29

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2024-39386

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Bridge: 13.0 - 14.1.1

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/bridge/apsb24-59.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1139/

Краткое описание: Обход безопасности в Microsoft Windows SmartScreen

Идентификатор уязвимости: CVE-2024-38180

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38180

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2024-38170

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

Уязвимый продукт: Microsoft Office LTSC 2021: 2021 for Mac
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.

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: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2024-38172

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

Уязвимый продукт: Microsoft Office LTSC 2021: 2021 for Mac
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.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-41831

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

33 **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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1133/

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-41830
BDU:2024-06333

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

34 **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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- http://www.talosintelligence.com/vulnerability_reports/TALOS-2024-2009
- https://bdu.fstec.ru/vul/2024-06333

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-39426

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

35 **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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1130/

Краткое описание: Повышение привилегий в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-39425

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-39424

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1134/

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-39423

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1136/

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-39422

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1135/

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2024-39383

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 24.002.20991
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

40

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-57.html

Краткое описание: Чтение локальных файлов в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-39399

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.4.4 - 2.4.7-p1
Magento Open Source: 2.4.4 - 2.4.7-p1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-61.html

42

Краткое описание: Межсайтовый скриптинг в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-39400

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.4.4 - 2.4.7-p1
Magento Open Source: 2.4.4 - 2.4.7-p1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Внедрение HTML-кода.

Последствия эксплуатации: Межсайтовый скриптинг

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:L/PR:H/UI:R/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-61.html

43

Краткое описание: Выполнение произвольного кода в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-39401

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.4.4 - 2.4.7-p1
Magento Open Source: 2.4.4 - 2.4.7-p1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-61.html

44

Краткое описание: Выполнение произвольного кода в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-39402

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.4.4 - 2.4.7-p1
Magento Open Source: 2.4.4 - 2.4.7-p1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-61.html

45

Краткое описание: Межсайтовый скриптинг в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-39403

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.4.4 - 2.4.7-p1
Magento Open Source: 2.4.4 - 2.4.7-p1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Внедрение HTML-кода.

Последствия эксплуатации: Межсайтовый скриптинг

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-61.html

Краткое описание: Запись локальных файлов в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2024-39397

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce): 2.4.4 - 2.4.7-p1
Magento Open Source: 2.4.4 - 2.4.7-p1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/magento/apsb24-61.html
- http://experienceleague.adobe.com/en/docs/commerce-knowledge-base/kb/troubleshooting/known-issues-patches-attached/security-update-available-for-adobe-commerce-apsb24-61

Краткое описание: Выполнение произвольного кода в Microsoft Windows Line Printer Daemon (LPD) Service

Идентификатор уязвимости: CVE-2024-38199

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Использование памяти после ее освобождения

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38199

Краткое описание: Выполнение произвольного кода в Zoom Workplace Apps and Rooms clients

Идентификатор уязвимости: CVE-2024-39825

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

Уязвимый продукт: Zoom Workplace Desktop App for Windows: 5.0.0 23168.0427 - 5.17.12
Zoom Workplace Desktop App for Linux: 5.1.418436.0628 - 5.17.11 3835
Zoom Workplace Desktop App for macOS: 5.0.0 23186.0427 - 5.17.11 31580
Zoom Workplace App for iOS: 5.0.0 23161.0427 - 5.17.11 14172
Zoom Workplace App for Android: 5.0.1 23478.0429 - 5.17.11 20383
Virtual Desktop Infrastructure (VDI): 5.0.1 - 5.17.12 24920
Zoom Rooms for Windows: до 6.0.0
Zoom Rooms for macOS: до 6.0.0 6108

Категория уязвимого продукта: Прикладное программное обеспечение

48

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://www.zoom.com/en/trust/security-bulletin/ZSB-24022/

Краткое описание: Выполнение произвольного кода в Microsoft Clipboard Virtual Channel Extension

Идентификатор уязвимости: CVE-2024-38131
BDU:2024-06351

Идентификатор программной ошибки: CWE-591 Хранение важных данных в некорректно заблокированной памяти

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Отправка специально сформированного запроса.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38131
- https://bdu.fstec.ru/vul/2024-06351

Краткое описание: Выполнение произвольного кода в Microsoft Windows TCP/IP

Идентификатор уязвимости: CVE-2024-38063
BDU:2024-06242

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38063
- https://bdu.fstec.ru/vul/2024-06242

51

Краткое описание: Выполнение произвольного кода в Microsoft Project

Идентификатор уязвимости: CVE-2024-38189
BDU:2024-06243

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office: 2016 - 2019
Microsoft Project: 2016 - 2019
Microsoft 365 Apps for Enterprise: 15.0.5589.1001 - 2306 16529.20182

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38189
- https://bdu.fstec.ru/vul/2024-06243

Краткое описание: Выполнение произвольного кода в Microsoft Windows Power Dependency Coordinator

Идентификатор уязвимости: CVE-2024-38107
BDU:2024-06329

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Использование памяти после ее освобождения

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38107
- https://bdu.fstec.ru/vul/2024-06329

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38154

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

53 **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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38154

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38121
BDU:2024-06323

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Подключение к вредоносному серверу.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38121
- https://bdu.fstec.ru/vul/2024-06323

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38128
BDU:2024-06273

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Подключение к вредоносному серверу.

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38128
- https://bdu.fstec.ru/vul/2024-06273

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38120
BDU:2024-06326

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

Уязвимый продукт: Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Подключение к вредоносному серверу.

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38120
- https://bdu.fstec.ru/vul/2024-06326

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-38130

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38130

58

Краткое описание: Повышение привилегий в Microsoft Windows kernel

Идентификатор уязвимости: CVE-2024-38106

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

Способ эксплуатации: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38106

Краткое описание: Выполнение произвольного кода в Microsoft Windows Scripting Engine

Идентификатор уязвимости: CVE-2024-38178
BDU:2024-06219

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.4037
Windows Server: до 2022 10.0.20348.2655

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-38178
- https://bdu.fstec.ru/vul/2024-06219

Краткое описание: Подделка запросов на стороне сервера в Tenable Security Center

Идентификатор уязвимости: CVE-2024-40898
BDU:2024-05368

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

Уязвимый продукт: SecurityCenter: до SC-202408.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Подделка запросов на стороне сервера

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-13
- https://bdu.fstec.ru/vul/2024-05368

Краткое описание: Отказ в обслуживании в Tenable Security Center

Идентификатор уязвимости: CVE-2024-38477
BDU:2024-05195

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SecurityCenter: до SC-202408.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Отказ в обслуживании

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: 7.5 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-13
- https://bdu.fstec.ru/vul/2024-05195

Краткое описание: Подделка запросов на стороне сервера в Tenable Security Center

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

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

Уязвимый продукт: SecurityCenter: до SC-202408.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Подделка запросов на стороне сервера

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: 9.0 AV:N/AC:H/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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-13
- https://bdu.fstec.ru/vul/2024-05131

63

Краткое описание: Выполнение произвольного кода в Tenable Security Center

Идентификатор уязвимости: CVE-2024-38475
BDU:2024-04936

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SecurityCenter: до SC-202408.1

Категория уязвимого продукта: Средства защиты информации

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: 8.1 AV:N/AC:H/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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-13
- https://bdu.fstec.ru/vul/2024-04936

Краткое описание: Отказ в обслуживании в Tenable Security Center

Идентификатор уязвимости: CVE-2024-36387
BDU:2024-05194

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: SecurityCenter: до SC-202408.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

64 **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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://www.tenable.com/security/tns-2024-13
- https://bdu.fstec.ru/vul/2024-05194

Краткое описание: Обход безопасности в SAP BusinessObjects Business Intelligence Platform

Идентификатор уязвимости: CVE-2024-41730
BDU:2024-06241

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: SAP BusinessObjects Business Intelligence suite: 4.3 - 4.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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: 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html
- https://bdu.fstec.ru/vul/2024-06241

Краткое описание: Получение конфиденциальной информации в SAP libraries

Идентификатор уязвимости: CVE-2023-49583
BDU:2023-08964

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: sap/xssec: до 3.6.0
sap/approuter: до 14.4.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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: 9.1 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2024.html
- https://bdu.fstec.ru/vul/2023-08964

Краткое описание: Получение конфиденциальной информации в SAP libraries

Идентификатор уязвимости: CVE-2023-50422
BDU:2023-08961

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: cloud-security-services-integration-library: 2.0.0 - 3.2.1
cloud-security-client-go: 0.1 - 0.16.0
sap/xssec: до 3.6.0
sap-xssec: до 4.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

67 **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: 9.1 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2024.html
- https://bdu.fstec.ru/vul/2023-08961

Краткое описание: Получение конфиденциальной информации в SAP libraries

Идентификатор уязвимости: CVE-2023-50423
BDU:2023-08962

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: cloud-security-services-integration-library: 2.0.0 - 3.2.1
cloud-security-client-go: 0.1 - 0.16.0
sap/xssec: до 3.6.0
sap-xssec: до 4.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

68 **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: 9.1 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2024.html
- https://bdu.fstec.ru/vul/2023-08962

Краткое описание: Получение конфиденциальной информации в SAP libraries

Идентификатор уязвимости: CVE-2023-50424
BDU:2023-08963

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: cloud-security-services-integration-library: 2.0.0 - 3.2.1
cloud-security-client-go: 0.1 - 0.16.0
sap/xssec: до 3.6.0
sap-xssec: до 4.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

69 **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: 9.1 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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2024.html
- https://bdu.fstec.ru/vul/2023-08963

Краткое описание: Получение конфиденциальной информации в Apache Traffic Server

Идентификатор уязвимости: CVE-2024-35161
BDU:2024-05796

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache Traffic Server: 8.0.0 - 9.2.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-08-12 / 2024-08-12

Ссылки на источник:

- http://lists.apache.org/thread/c4mcmpblgl8kkmyt56t23543gp8v56m0
- https://bdu.fstec.ru/vul/2024-05796

Краткое описание: Получение конфиденциальной информации в Apache Traffic Server

Идентификатор уязвимости: CVE-2023-38522
BDU:2024-05797

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache Traffic Server: 8.0.0 - 9.2.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 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: 2024-08-12 / 2024-08-12

Ссылки на источник:

- http://lists.apache.org/thread/c4mcmpblgl8kkmyt56t23543gp8v56m0
- https://bdu.fstec.ru/vul/2024-05797

Краткое описание: Выполнение произвольного кода в Delta Electronics DIAScreen

Идентификатор уязвимости: CVE-2024-7502

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: DIAScreen: до 1.4.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

72 **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: 2024-08-12 / 2024-08-12

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-219-01

Краткое описание: Выполнение произвольного кода в Jenkins and Jenkins LTS

Идентификатор уязвимости: CVE-2024-43044
BDU:2024-06145

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Jenkins: 2.0 - 2.470
Jenkins LTS: 2.7.1 - 2.452.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

73 **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: 2024-08-12 / 2024-08-12

Ссылки на источник:

- http://www.jenkins.io/security/advisory/2024-08-07/#SECURITY-3430
- https://bdu.fstec.ru/vul/2024-06145