НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-09-15.1 | 15 сентября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2025-40804	Siemens SIMATIC Virtualization as a Service (SIVaaS)	Сетевой	OSI	2025-09-12	✗
2	Высокая	CVE-2025-40798	Siemens User Management Component (UMC)	Сетевой	DoS	2025-09-12	✓
3	Высокая	CVE-2025-40797	Siemens User Management Component (UMC)	Сетевой	DoS	2025-09-12	✓
4	Высокая	CVE-2025-40796	Siemens User Management Component (UMC)	Сетевой	DoS	2025-09-12	✓
5	Критическая	CVE-2025-40795	Siemens User Management Component (UMC)	Сетевой	ACE	2025-09-12	✓
6	Высокая	CVE-2025-10200	Microsoft Edge	Сетевой	ACE	2025-09-12	✓
7	Высокая	CVE-2025-10201	Microsoft Edge	Сетевой	OSI	2025-09-12	✓
8	Высокая	CVE-2025-58060	CUPS	Локальный	SB	2025-09-11	✓
9	Высокая	CVE-2025-6454	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	CSRF	2025-09-11	✓
10	Высокая	CVE-2025-2256	GitLab Community Edition (CE) and Enterprise Edition (EE)	Сетевой	DoS	2025-09-11	✓
11	Критическая	CVE-2025-55232	Microsoft High Performance Compute (HPC) Pack	Сетевой	ACE	2025-09-09	✓

12	Высокая	CVE-2025-10201	Google Chrome	Сетевой	OSI	2025-09-09	✓
13	Высокая	CVE-2025-10200	Google Chrome	Сетевой	ACE	2025-09-09	✓
14	Высокая	CVE-2025-54242	Adobe Premiere Pro	Локальный	ACE	2025-09-09	✓
15	Высокая	CVE-2025-54260	Adobe Substance 3D Modeler	Локальный	OSI	2025-09-09	✓
16	Высокая	CVE-2025-54259	Adobe Substance 3D Modeler	Локальный	ACE	2025-09-09	✓
17	Высокая	CVE-2025-54258	Adobe Substance 3D Modeler	Локальный	ACE	2025-09-09	✓
18	Высокая	CVE-2025-54245	Adobe Substance 3D Viewer	Локальный	ACE	2025-09-09	✓
19	Высокая	CVE-2025-54244	Adobe Substance 3D Viewer	Локальный	ACE	2025-09-09	✓
20	Высокая	CVE-2025-54243	Adobe Substance 3D Viewer	Локальный	ACE	2025-09-09	✓
21	Высокая	CVE-2025-54113	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2025-09-09	✓
22	Высокая	CVE-2025-54106	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2025-09-09	✓
23	Высокая	CVE-2025-54257	Adobe Acrobat and Reader	Локальный	ACE	2025-09-09	✓
24	Высокая	CVE-2025-9872	Ivanti Endpoint Manager	Сетевой	WLF	2025-09-09	✓
25	Высокая	CVE-2025-9712	Ivanti Endpoint Manager	Сетевой	WLF	2025-09-09	✓

1

Краткое описание: Получение конфиденциальной информации в Siemens SIMATIC Virtualization as a Service (SIVaaS)

Идентификатор уязвимости: CVE-2025-40804

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: SIMATIC Virtualization as a Service (SIVaaS):
все версии

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-534283.html
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-254-02

Краткое описание: Отказ в обслуживании в Siemens User Management Component (UMC)

Идентификатор уязвимости: CVE-2025-40798

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SIMATIC PCS neo:
4.1 - 5.0
User Management Component (UMC):
до 2.15.1.3

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-722410.html
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-254-07

Краткое описание: Отказ в обслуживании в Siemens User Management Component (UMC)

Идентификатор уязвимости: CVE-2025-40797

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SIMATIC PCS neo:
4.1 - 5.0
User Management Component (UMC):
до 2.15.1.3

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-722410.html
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-254-07

Краткое описание: Отказ в обслуживании в Siemens User Management Component (UMC)

Идентификатор уязвимости: CVE-2025-40796

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SIMATIC PCS neo:
4.1 - 5.0
User Management Component (UMC):
до 2.15.1.3

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Отказ в обслуживании

4 **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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-722410.html
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-254-07

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

Идентификатор уязвимости: CVE-2025-40795

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: SIMATIC PCS neo:
4.1 - 5.0
User Management Component (UMC):
до 2.15.1.3

Категория уязвимого продукта: Не определено

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

5 **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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-722410.html
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-254-07

6

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-10200

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 140.0.3485.54

Категория уязвимого продукта: Операционные системы Microsoft 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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-10200

7

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2025-10201

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

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 140.0.3485.54

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 4.8 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-12 / 2025-09-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-10201

8

Краткое описание: Обход безопасности в CUPS

Идентификатор уязвимости: CVE-2025-58060

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: cups:
2.2.0 - 2.4.12

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированного запроса.

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

Оценка CVSSv4: 5.2 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-11 / 2025-09-11

Ссылки на источник:

- https://github.com/OpenPrinting/cups/security/advisories/GHSA-4c68-qgrh-rmmq

9

Краткое описание: Подделка запросов на стороне сервера в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2025-6454

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

Уязвимый продукт: Gitlab Community Edition:
16.11.0 - 18.3.1
GitLab Enterprise Edition:
16.11.0 - 18.3.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Подделка запросов на стороне сервера

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

Оценка CVSSv4: 1.3 AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-11 / 2025-09-11

Ссылки на источник:

- https://about.gitlab.com/releases/2025/09/10/patch-release-gitlab-18-3-2-released/

10

Краткое описание: Отказ в обслуживании в GitLab Community Edition (CE) and Enterprise Edition (EE)

Идентификатор уязвимости: CVE-2025-2256

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Gitlab Community Edition:
7.12 - 18.3.1
GitLab Enterprise Edition:
7.12.0 - 18.3.1

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-11 / 2025-09-11

Ссылки на источник:

- https://about.gitlab.com/releases/2025/09/10/patch-release-gitlab-18-3-2-released/

11

Краткое описание: Выполнение произвольного кода в Microsoft High Performance Compute (HPC) Pack

Идентификатор уязвимости: CVE-2025-55232
BDU:2025-10917

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft HPC Pack:
2019

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55232
- https://bdu.fstec.ru/vul/2025-10917

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-10201

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

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 140.0.7339.81

Категория уязвимого продукта: Не определено

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

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.

12

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

Оценка CVSSv4: 4.8 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_9.html
- https://crbug.com/439305148

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-10200

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 140.0.7339.81

Категория уязвимого продукта: Не определено

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.

13

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_9.html
- https://crbug.com/440454442

14

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2025-54242

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Premiere Pro:
22.0 - 25.3

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/premiere_pro/apsb25-87.html

15

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Modeler

Идентификатор уязвимости: CVE-2025-54260

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Substance 3D Modeler:
1.1 - 1.22.2

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-92.html

16

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Modeler

Идентификатор уязвимости: CVE-2025-54259

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

Уязвимый продукт: Adobe Substance 3D Modeler:
1.1 - 1.22.2

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-92.html

17

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Modeler

Идентификатор уязвимости: CVE-2025-54258

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Substance 3D Modeler: 1.1 - 1.22.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-92.html

18

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Viewer

Идентификатор уязвимости: CVE-2025-54245

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Viewer: 0.9.1 - 0.25.1

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-89.html

19

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Viewer

Идентификатор уязвимости: CVE-2025-54244

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

Уязвимый продукт: Adobe Substance 3D Viewer:
0.9.1 - 0.25.1

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-89.html

20

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Viewer

Идентификатор уязвимости: CVE-2025-54243

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Viewer: 0.9.1 - 0.25.1

Категория уязвимого продукта: Не определено

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-89.html

21

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

Идентификатор уязвимости: CVE-2025-54113
BDU:2025-10938

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

Уязвимый продукт: Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.4946

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-54113
- https://bdu.fstec.ru/vul/2025-10938

22

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

Идентификатор уязвимости: CVE-2025-54106

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

Уязвимый продукт: Windows Server:
2012 Gold - 2025 10.0.26100.4946

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-54106

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2025-54257

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat:
15.006.30306 - 2025.001.20630
Adobe Reader:
20.001.30002 - 25.001.20672

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb25-85.html

Краткое описание: Запись локальных файлов в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2025-9872

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

Уязвимый продукт: Endpoint Manager:
2022 - 2024 January-2025 Update

Категория уязвимого продукта: Не определено

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.

24

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-September-2025-for-Ivanti-EPM-2024-SU3-and-EPM-2022-SU8?language=en_US&_gl=1*1czhpgc*_gcl_au*NzkxMzg0ODIwLjE3NTc0MzQyMDE.

Краткое описание: Запись локальных файлов в Ivanti Endpoint Manager

Идентификатор уязвимости: CVE-2025-9712

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

Уязвимый продукт: Endpoint Manager:
2022 - 2024 January-2025 Update

Категория уязвимого продукта: Не определено

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.

25

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-09 / 2025-09-09

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-September-2025-for-Ivanti-EPM-2024-SU3-and-EPM-2022-SU8?language=en_US&_gl=1*1czhpgc*_gcl_au*NzkxMzg0ODIwLjE3NTc0MzQyMDE.