НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-27.1 | 27 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-7102	Barracuda Email Security Gateway Appliance (ESG)	Сетевой	ACE	2023-12-27	✓
2	Высокая	CVE-2023-49933	SchedMD Slurm	Сетевой	OSI	2023-12-26	✓
3	Высокая	CVE-2023-49938	SchedMD Slurm	Сетевой	RLF	2023-12-26	✓
4	Критическая	CVE-2023-49937	SchedMD Slurm	Сетевой	ACE	2023-12-26	✓
5	Высокая	CVE-2023-49936	SchedMD Slurm	Сетевой	DoS	2023-12-26	✓
6	Высокая	CVE-2023-49935	SchedMD Slurm	Сетевой	OSI	2023-12-26	✓
7	Высокая	CVE-2023-44487	Ingress-NGINX Controller for Kubernetes	Сетевой	DoS	2023-12-26	✓
8	Высокая	CVE-2023-42833	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2023-12-26	✓
9	Критическая	CVE-2023-49934	SchedMD Slurm	Сетевой	ACE	2023-12-26	✓
10	Высокая	CVE-2023-40414	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2023-12-26	✓
11	Высокая	CVE-2023-42866	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2023-12-26	✓
12	Высокая	CVE-2023-37197	Schneider Electric	Сетевой	CI	2023-07-12	✓
13	Высокая	CVE-2023-37196	Schneider Electric	Сетевой	CI	2023-07-12	✓

14	Критическая	CVE-2023-39001	OPNsense Community Edition и Business Edition	Сетевой	ACE	2023-09-08	✓
15	Критическая	CVE-2023-38997	OPNsense Community Edition и Business Edition	Сетевой	PE	2023-09-08	✓

Краткое описание: Выполнение произвольного кода в Barracuda Email Security Gateway Appliance (ESG)

Идентификатор уязвимости: CVE-2023-7102

Идентификатор программной ошибки: CWE-749 Доступны опасные методы или функции

Уязвимый продукт: Email Security Gateway (ESG): 5.1.3 - 9.2.1.001

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-27 / 2023-12-27

Ссылки на источник:

- http://www.barracuda.com/company/legal/esg-vulnerability
- http://www.cve.org/CVERecord?id=CVE-2023-7101
- http://metacpan.org/dist/Spreadsheet-ParseExcel
- http://github.com/haile01/perl_spreadsheet_excel_rce_poc
- http://github.com/jmcnamara/spreadsheet-parseexcel/blob/c7298592e102a375d43150cd002feed806557c15/lib/Spreadsheet/ParseExcel/Utility.pm#L171
- http://github.com/mandiant/Vulnerability-Disclosures/blob/master/2023/MNDT-2023-0019.md

2

Краткое описание: Получение конфиденциальной информации в SchedMD Slurm

Идентификатор уязвимости: CVE-2023-49933

Идентификатор программной ошибки: CWE-924 Некорректная проверка целостности сообщения, полученного по каналу связи

Уязвимый продукт: Slurm: 22.05.0.1 - 23.11.0.1

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: 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: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

3

Краткое описание: Чтение локальных файлов в SchedMD Slurm

Идентификатор уязвимости: CVE-2023-49938

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Slurm: 22.05.0.1 - 23.02.6.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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:H/I:L/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

4

Краткое описание: Выполнение произвольного кода в SchedMD Slurm

Идентификатор уязвимости: CVE-2023-49937

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Slurm: 22.05.0.1 - 23.11.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

Краткое описание: Отказ в обслуживании в SchedMD Slurm

Идентификатор уязвимости: CVE-2023-49936

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Slurm: 22.05.0.1 - 23.11.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

6

Краткое описание: Получение конфиденциальной информации в SchedMD Slurm

Идентификатор уязвимости: CVE-2023-49935

Идентификатор программной ошибки: CWE-613 Некорректно настроенный срок действия сессий

Уязвимый продукт: Slurm: 23.02.0.1 - 23.11.0.1

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: 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: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

7

Краткое описание: Отказ в обслуживании в Ingress-NGINX Controller for Kubernetes

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Ingress-NGINX Controller for Kubernetes: 1.0.0 - 1.9.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

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: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.9.5
- https://bdu.fstec.ru/vul/2023-06559

Краткое описание: Выполнение произвольного кода в WebKitGTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2023-42833

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

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://support.apple.com/en-us/HT213940

Краткое описание: Выполнение произвольного кода в SchedMD Slurm

Идентификатор уязвимости: CVE-2023-49934

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

Уязвимый продукт: Slurm: 23.11.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

Краткое описание: Выполнение произвольного кода в WebKitGTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2023-40414

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Последствия эксплуатации: выполнение произвольного кода

10

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

Оценка CVSSv3: 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: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://support.apple.com/en-us/HT213940

Краткое описание: Выполнение произвольного кода в WebKitGTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2023-42866

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

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Последствия эксплуатации: выполнение произвольного кода

11

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-26 / 2023-12-26

Ссылки на источник:

- http://support.apple.com/en-us/HT213843

Краткое описание: Внедрение кода в Schneider Electric

Идентификатор уязвимости: CVE-2023-37197

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

Уязвимый продукт: StruxureWare Data Center Expert: до 7.9.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: внедрение кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-19

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-37197
- https://bdu.fstec.ru/vul/2023-03694

Краткое описание: Внедрение кода в Schneider Electric

Идентификатор уязвимости: CVE-2023-37196

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

Уязвимый продукт: StruxureWare Data Center Expert: до 7.9.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: внедрение кода

13 **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: 2023-07-12 / 2023-07-19

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-37196
- https://bdu.fstec.ru/vul/2023-03626

14

Краткое описание: Выполнение произвольного кода в OPNsense Community Edition и Business Edition

Идентификатор уязвимости: CVE-2023-39001

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

Уязвимый продукт: OPNsense Community Edition: до 23.7
OPNsense Business Edition: до 23.4.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка 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: 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: 2023-09-08 / 2023-10-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-39001

Краткое описание: Повышение привилегий в OPNsense Community Edition и Business Edition

Идентификатор уязвимости: CVE-2023-38997

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

Уязвимый продукт: OPNsense Community Edition: до 23.7
OPNsense Business Edition: до 23.4.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: повышение привилегий

15

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

Оценка CVSSv3: 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: 2023-09-08 / 2023-10-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38997