НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-29.1 | 29 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-7163	D-Link D-View	Сетевой	OSI	2023-12-28	✓
2	Высокая	CVE-2022-43680	Apache OpenOffice	Сетевой	DoS	2023-12-28	✓
3	Высокая	CVE-2023-47804	Apache OpenOffice	Сетевой	ACE	2023-12-28	✓
4	Высокая	CVE-2023-32233	Juniper Secure Analytics (JSA)	Локальный	ACE	2023-12-28	✓
5	Высокая	CVE-2023-35001	Juniper Secure Analytics (JSA)	Локальный	ACE	2023-12-28	✓
6	Высокая	CVE-2023-36478	Juniper Secure Analytics (JSA)	Сетевой	DoS	2023-12-28	✓
7	Критическая	CVE-2023-40787	Juniper Secure Analytics (JSA)	Сетевой	ACE	2023-12-28	✓
8	Высокая	CVE-2023-41835	Juniper Secure Analytics (JSA)	Сетевой	DoS	2023-12-28	✓
9	Высокая	CVE-2023-44487	Juniper Secure Analytics (JSA)	Сетевой	DoS	2023-12-28	✓
10	Высокая	CVE-2023-46589	Juniper Secure Analytics (JSA)	Сетевой	XSS\CSS	2023-12-28	✓
11	Критическая	CVE-2023-46604	HPE Intelligent Management Center и Juniper Secure Analytics (JSA)	Сетевой	ACE	2023-12-28	✓

1

Краткое описание: Получение конфиденциальной информации в D-Link D-View

Идентификатор уязвимости: CVE-2023-7163

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

Уязвимый продукт: D-View: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2023-43

2

Краткое описание: Отказ в обслуживании в Apache OpenOffice

Идентификатор уязвимости: CVE-2022-43680

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenOffice: 4.0.0 - 4.1.14

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://cwiki.apache.org/confluence/display/OOOUSERS/AOO+4.1.15+Release+Notes
- https://bdu.fstec.ru/vul/2023-02688

3

Краткое описание: Выполнение произвольного кода в Apache OpenOffice

Идентификатор уязвимости: CVE-2023-47804

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: OpenOffice: 4.0.0 - 4.1.14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://seclists.org/oss-sec/2023/q4/343
- http://cwiki.apache.org/confluence/display/OOOUSERS/AOO+4.1.15+Release+Notes

4

Краткое описание: Выполнение произвольного кода в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-32233

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

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: 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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-02625

5

Краткое описание: Выполнение произвольного кода в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-35001

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

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: 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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-03778

Краткое описание: Отказ в обслуживании в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-36478

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

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

6 **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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved

7

Краткое описание: Выполнение произвольного кода в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-40787

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

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

Оценка CVSSv3: 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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved

8

Краткое описание: Отказ в обслуживании в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-41835

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

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

Категория уязвимого продукта: Средства защиты информации

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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-08554

9

Краткое описание: Отказ в обслуживании в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-44487

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

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

Категория уязвимого продукта: Средства защиты информации

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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-06559

Краткое описание: Межсайтовый скриптинг в Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-46589

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: межсайтовый скриптинг

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: 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: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved

11

Краткое описание: Выполнение произвольного кода в HPE Intelligent Management Center и Juniper Secure Analytics (JSA)

Идентификатор уязвимости: CVE-2023-46604

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: HP Intelligent Management Center: до 7.3 E0710H02
Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP7 IF02

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-28 / 2023-12-28

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04574en_us
- http://supportportal.juniper.net/s/article/2023-12-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved
- https://bdu.fstec.ru/vul/2023-07372