

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

## Бюллетень об уязвимостях программного обеспечения

VULN.2023-10-23.1 | 23 октября 2023 года

TLP: WHITE



## Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-44194	Juniper Junos OS	Локальный	PE	2023-10-23	✓
2	Высокая	CVE-2023-4601	National Instruments Measurement & Automation Explorer	Сетевой	ACE	2023-10-20	✓
3	Высокая	CVE-2023-35186	SolarWinds Access Rights Manager	Смежная сеть	ACE	2023-10-20	✓
4	Высокая	CVE-2023-35185	SolarWinds Access Rights Manager	Смежная сеть	ACE	2023-10-20	✓
5	Высокая	CVE-2023-35182	SolarWinds Access Rights Manager	Смежная сеть	ACE	2023-10-20	✓
6	Высокая	CVE-2023-35184	SolarWinds Access Rights Manager	Смежная сеть	ACE	2023-10-20	✓
7	Высокая	CVE-2023-35183	SolarWinds Access Rights Manager	Локальный	RLF	2023-10-20	✓
8	Высокая	CVE-2023-35181	SolarWinds Access Rights Manager	Локальный	RLF	2023-10-20	✓
9	Высокая	CVE-2023-35180	SolarWinds Access Rights Manager	Смежная сеть	ACE	2023-10-20	✓
10	Высокая	CVE-2023-35187	SolarWinds Access Rights Manager	Смежная сеть	ACE	2023-10-20	✓
11	Высокая	CVE-2023-34052	VMware Aria Operations for Logs (formerly vRealize Log Insight)	Сетевой	ACE	2023-10-20	✓

12	Высокая	CVE-2023-34051	VMware Aria Operations for Logs (formerly vRealize Log Insight)	Сетевой	ACE	2023-10-20	✓
13	Высокая	CVE-2023-44833	D-Link DIR-823G	Сетевой	DoS	2023-10-05	✗
14	Критическая	CVE-2023-44807	D-Link DIR-820L	Сетевой	ACE	2023-10-10	✗
15	Высокая	CVE-2023-45208	D-Link DAP-X1860 repeate	Смежная сеть	ACE	2023-10-10	✗
16	Высокая	CVE-2023-44959	D-Link DSL-3782	Сетевой	PE	2023-10-09	✗
17	Высокая	CVE-2023-25607	Fortinet FortiManager, FortiAnalyzer and FortiADC	Локальный	ACE	2023-10-12	✓
18	Высокая	CVE-2023-41679	Fortinet FortiManager	Сетевой	ACE	2023-10-12	✓

**Краткое описание:** Повышение привилегий в Juniper Junos OS

**Идентификатор уязвимости:** CVE-2023-44194

**Идентификатор программной ошибки:** CWE-276 Некорректные разрешения, назначаемые по умолчанию

**Уязвимый продукт:** Juniper Junos OS: 20.1 - 21.4R3

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

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** повышение привилегий

1 **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:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-23 / 2023-10-23

**Ссылки на источник:**

- <http://supportportal.juniper.net/JSA73158>

**Краткое описание:** Выполнение произвольного кода в National Instruments Measurement & Automation Explorer

**Идентификатор уязвимости:** CVE-2023-4601

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** National Instruments Measurement & Automation Explorer: 2023 Q3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

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:** 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:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.ni.com/en/support/documentation/supplemental/23/stack-based-buffer-overflow-in-ni-system-configuration.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1568/>

**Краткое описание:** Выполнение произвольного кода в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35186

**Идентификатор программной ошибки:** CWE-502 Десериализация недоверенных данных

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35186>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1566/>

**Краткое описание:** Выполнение произвольного кода в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35185

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

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально созданных HTTP-запросов.

**Последствия эксплуатации:** выполнение произвольного кода

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35185>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1565/>

**Краткое описание:** Выполнение произвольного кода в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35182

**Идентификатор программной ошибки:** CWE-502 Десериализация недоверенных данных

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35182>
- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1564/>
- <https://bdu.fstec.ru/vul/2023-07002>



**Краткое описание:** Выполнение произвольного кода в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35184

**Идентификатор программной ошибки:** CWE-502 Десериализация недоверенных данных

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** выполнение произвольного кода

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35184>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1563/>

Краткое описание: Чтение локальных файлов в SolarWinds Access Rights Manager

Идентификатор уязвимости: CVE-2023-35183

Идентификатор программной ошибки: CWE-276 Некорректные разрешения, назначаемые по умолчанию

Уязвимый продукт: SolarWinds Access Rights Manager: до 2023.2.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: чтение локальных файлов

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: 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: 2023-10-20 / 2023-10-20

Ссылки на источник:

- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35183>
- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1562/>

**Краткое описание:** Чтение локальных файлов в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35181

**Идентификатор программной ошибки:** CWE-276 Некорректные разрешения, назначаемые по умолчанию

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** чтение локальных файлов

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:** 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:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35181>
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1561/>

**Краткое описание:** Выполнение произвольного кода в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35180

**Идентификатор программной ошибки:** CWE-502 Десериализация недоверенных данных

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35180>
- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1560/>

**Краткое описание:** Выполнение произвольного кода в SolarWinds Access Rights Manager

**Идентификатор уязвимости:** CVE-2023-35187

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

**Уязвимый продукт:** SolarWinds Access Rights Manager: до 2023.2.1

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально созданных HTTP-запросов.

**Последствия эксплуатации:** выполнение произвольного кода

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

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35187>
- [http://documentation.solarwinds.com/en/success\\_center/arm/content/release\\_notes/arm\\_2023-2-1\\_release\\_notes.htm](http://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm)
- <http://www.zerodayinitiative.com/advisories/ZDI-23-1567/>

**Краткое описание:** Выполнение произвольного кода в VMware Aria Operations for Logs (formerly vRealize Log Insight)

**Идентификатор уязвимости:** CVE-2023-34052

**Идентификатор программной ошибки:** CWE-502 Десериализация недоверенных данных

**Уязвимый продукт:** VMware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**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:** 8.1 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:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.vmware.com/security/advisories/VMSA-2023-0021.html>
- <http://www.vmware.com/security/advisories/VMSA-2023-00210.html>

**Краткое описание:** Выполнение произвольного кода в VMware Aria Operations for Logs (formerly vRealize Log Insight)

**Идентификатор уязвимости:** CVE-2023-34051

**Идентификатор программной ошибки:** CWE-287 Некорректная аутентификация

**Уязвимый продукт:** VMware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход процесса аутентификации

**Последствия эксплуатации:** выполнение произвольного кода

12

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

**Оценка CVSSv3:** 8.1 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:** 2023-10-20 / 2023-10-20

**Ссылки на источник:**

- <http://www.vmware.com/security/advisories/VMSA-2023-0021.html>
- <http://www.vmware.com/security/advisories/VMSA-2023-00210.html>

**Краткое описание:** Отказ в обслуживании в D-Link DIR-823G

**Идентификатор уязвимости:** CVE-2023-44833

**Идентификатор программной ошибки:** CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

**Уязвимый продукт:** D-Link DIR-823G: A1V1.0.2B05

**Категория уязвимого продукта:** Средства защиты информации

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** отказ в обслуживании

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

**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:** 2023-10-05 / 2023-10-06

**Ссылки на источник:**

- <https://nvd.nist.gov/vuln/detail/CVE-2023-44833>
- <https://bdu.fstec.ru/vul/2023-06399>



Краткое описание: Выполнение произвольного кода в D-Link DIR-820L

Идентификатор уязвимости: CVE-2023-44807

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link DIR-820L: 1.05B03

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-10 / 2023-10-16

Ссылки на источник:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-44807>
- <https://bdu.fstec.ru/vul/2023-06451>

**Краткое описание:** Выполнение произвольного кода в D-Link DAP-X1860 repeate

**Идентификатор уязвимости:** CVE-2023-45208

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

**Уязвимый продукт:** D-Link DAP-X1860 repeate: до 1.01b05-01

**Категория уязвимого продукта:** Средства защиты информации

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** выполнение произвольного кода

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

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2023-10-10 / 2023-10-16

**Ссылки на источник:**

- <https://nvd.nist.gov/vuln/detail/CVE-2023-45208>
- <https://bdu.fstec.ru/vul/2023-06612>

**Краткое описание:** Повышение привилегий в D-Link DSL-3782

**Идентификатор уязвимости:** CVE-2023-44959

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

**Уязвимый продукт:** D-Link DSL-3782: до 1.03

**Категория уязвимого продукта:** Средства защиты информации

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** повышение привилегий

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

**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:** 2023-10-09 / 2023-10-11

**Ссылки на источник:**

- <https://nvd.nist.gov/vuln/detail/CVE-2023-44959>
- <https://bdu.fstec.ru/vul/2023-06564>

**Краткое описание:** Выполнение произвольного кода в Fortinet FortiManager, FortiAnalyzer and FortiADC

**Идентификатор уязвимости:** CVE-2023-25607

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

**Уязвимый продукт:** Fortinet FortiManager, FortiAnalyzer and FortiADC:  
FortiAnalyzer: 6.0.0 - 7.2.2  
FortiManager: 6.0.0 - 7.2.2  
FortiADC: 6.0.0 - 7.1.0

**Категория уязвимого продукта:** Средства защиты информации

**Способ эксплуатации:** Отправка специально сформированных данных.

17 **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:** 2023-10-12 / 2023-10-12

**Ссылки на источник:**

- <http://fortiguard.com/psirt/FG-IR-22-352>
- <https://bdu.fstec.ru/vul/2023-06696>

Краткое описание: Выполнение произвольного кода в Fortinet FortiManager

Идентификатор уязвимости: CVE-2023-41679

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Fortinet FortiManager: 6.0.0 - 7.2.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

18

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

Оценка CVSSv3: 8.5 AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-12 / 2023-10-12

Ссылки на источник:

- <http://fortiguard.com/psirt/FG-IR-23-062>
- <https://bdu.fstec.ru/vul/2023-06708>