

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220901.25 | 1 сентября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в AVEVA Edge

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	AVEVA Edge: 2020 R2 SP1
Дата выявления	26 августа 2022 г.
Дата обновления	26 августа 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-36970	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректным предупреждением об опасных операциях.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-357: Недостаточно очевидное предупреждение об опасных операциях</p> <p>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.</p>	8.8

<p>MITRE: CVE-2022-28685</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-502: Десериализация недоверенных данных</p> <p>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.</p>	<p>8.8</p>
<p>MITRE: CVE-2022-28686 CVE-2022-28687 CVE-2022-28688</p>	<p>Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена небезопасной загрузкой DLL-библиотеки.</p> <p>CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-427: Неконтролируемый элемент пути поиска</p> <p>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.</p>	<p>8.0</p>
<p>MITRE: CVE-2022-36969</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-611: Некорректное ограничение ссылок на внешние сущности XML</p> <p>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.</p>	<p>8.1</p>

Ссылки на
источники

http://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2022-005.pdf