

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220511.11 | 11 мая 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в Avaya switches

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	ERS3500: Все версии ERS3600: Все версии ERS4900: Все версии ERS5900: Все версии
Дата выявления	03 мая 2022 г.
Дата обновления	03 мая 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-29860	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.  CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C  CWE-122: Переполнение буфера в динамической памяти	9.8

	<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>MITRE: CVE-2022-29861</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-121: Переполнение буфера в стеке</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>9.8</p>

Ссылки на  
источники

<http://www.armis.com/blog/tlstorm-2-nanossl-tls-library-misuse-leads-to-vulnerabilities-in-common-switches/>