

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221110.6 | 10 ноября 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Citrix Access Gateway

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Citrix Access Gateway: до 12.1.65.21 Citrix Netscaler ADC: до 12.1-55.289
Дата выявления	8 ноября 2022 г.
Дата обновления	8 ноября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-27510	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации в целевой системе и получить несанкционированный доступ к ней. Уязвимость актуальна только для Citrix Gateway настроенного как VPN.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-287: Некорректная аутентификация</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>	9.8

MITRE: CVE-2022-27513	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к удаленному рабочему столу пользователя посредством фишинговой атаки на него. Уязвимость актуальна только для Citrix Gateway настроенного как VPN с функцией прокси RDP.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H</p> <p>CWE-345: Некорректная проверка достоверности 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>	8.3
Ссылки на источники	http://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516	