НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200914.4 | 14 сентября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Jabber для Windows

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Jabber для Windows до следующих версий: 12.1.3, 12.5.2 ,12.6.3, 12.7.2, 12.8.3, 12.9.1
Дата выявления	2 сентября 2020 г.
Дата обновления	2 сентября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3495	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сообщения по протоколу XMPP. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	9.9

MITRE: CVE-2020-3430	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой входных данных в приложении обработки протоколов. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение.	8.8
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020090312 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-UyTKCPGg https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-vY8M4KGB	