НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221116.9 | 16 ноября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в компоненте AMaViS Zimbra Collaboration (ZCS).

Идентификатор уязвимости	MITRE: CVE-2022-41352
Идентификатор программной ошибки	CWE-254: Уязвимости в безопасности ПО
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольный код в целевой системе посредством отправки специально созданного вредоносного архива. Уязвимость обусловлена некорректным извлечением файлов для сканирования.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	AMaViS: 2.1.0 - 2.12.2
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.
Дата выявления	8 октября 2022 г.
Дата обновления	13 ноября 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)

Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	http://forums.zimbra.org/viewtopic.php?t=71153&p=306532 http://blog.zimbra.com/2022/09/security-update-make-sure-to-install-pax-spax/