НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200514.6| 14 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в OpenSMTPD

Идентификатор уязвимости	MITRE: CVE-2020-8794
Идентификатор программной ошибки	CWE-125: Чтение за пределами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного почтового сообщения. Уязвимость обусловлена некорректной обработкой ответов от SMTP-сервера в функции mta_io.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	OpenSMTPD до v6.6.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	25 февраля 2020 г.
Дата обновления	26 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.openwall.com/lists/oss-security/2020/02/24/5 https://nvd.nist.gov/vuln/detail/CVE-2020-8794 https://blog.trendmicro.com/trendlabs-security-intelligence/opensmtpd-vulnerability-cve-2020-8794-can-lead-to-root-privilege-escalation-and-remote-code-execution/