НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200203.2 | 3 февраля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение команд в ПО OpenSMTPD

Идентификатор уязвимости	MITRE: CVE-2020-7247
Идентификатор программной ошибки	CWE-252: Отсутствует проверка возвращаемых значений
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе от имени суперпользователя. Уязвимость обусловлена некорректной проверкой адресов электронной почты SMTP-сервером.
Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимое ПО	OpenSMTPD v6.6 и ранее
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	29 января 2020 г.
Дата обновления	31 января 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/E:P/RL:O/RC:C
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 (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://www.debian.org/security/2020/dsa-4611 https://www.openwall.com/lists/oss-security/2020/01/28/3 https://packetstormsecurity.com/files/156145/OpenSMTPD-6.6.2-Remote-Code-Execution.html