НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200522.2| 22 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Обход процесса аутентификации в Zoho ManageEngine ServiceDesk Plus

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе. Уязвимость обусловлена некорректной реализацией механизма аутентификации по протоколу OAuth.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Zoho ManageEngine ServiceDesk Plus до v11.1 сборка 11115
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 мая 2020 г.
Дата обновления	20 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Удаленный (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.manageengine.com/products/service-desk/on-premises/readme.html?112233 https://www.cybersecurity-help.cz/vdb/SB2020052027