НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200921.1 | 21 сентября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Zoho ManageEngine Desktop Central

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Zoho ManageEngine Desktop Central до v10.0.570, v10.0.574
Дата выявления	15 сентября 2020 г.
Дата обновления	15 сентября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством отправки специально сформированного запроса на аутентификацию. Уязвимость обусловлена некорректной обработкой запросов аутентификации при обмене данными между агентом и сервером. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена целочисленным переполнением буфера памяти при обработке входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение.	9.8
MITRE: Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена некорректным применением ограничений безопасности при обработке сообщений, полученных от агента. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение.	9.8

Ссылки на источники	https://www.manageengine.com/products/desktop-central/hotfix-readme1.html# https://www.cybersecurity-help.cz/vdb/SB2020091515 https://www.cybersecurity-help.cz/vdb/SB2020091514