

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220124.37 | 24 января 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Zoho ManageEngine OpManager

Категория уязвимого продукта	Прикладное программное обеспечение	
Уязвимый продукт	Zoho ManageEngine OpManager: до 12.5 125490	
Дата выявления	17 января 2022 г.	
Дата обновления	17 января 2022 г.	
Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
Не определен	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	9.8

Не определен	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольный файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C</p> <p>CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	7.5
--------------	---	-----

Ссылки на источники	http://www.manageengine.com/network-monitoring/help/read-me-complete.html#125459 https://www.cybersecurity-help.cz/vdb/SB2022011718
---------------------	--