НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220812.25 | 12 августа 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Dell Enterprise Hybrid Cloud

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Dell Enterprise Hybrid Cloud: до 4.1.2
Дата выявления	11 августа 2022 г.
Дата обновления	11 августа 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-31660 CVE-2022-31661 CVE-2022-31664	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с привилегиями «root» в целевой системе. Уязвимость обусловлена некорректным управлением привилегиями. CVSSv3.0: AV:L/AC:L/PR:L/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: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.8

MITRE: CVE-2022-31662	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольные файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.5
MITRE: CVE-2022-31656	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена ошибкой в процессе проверки подлинности. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	10.0
MITRE: CVE-2022-31675	Эксплуатация уязвимости позволяет удаленному злоумышленнику создать пользователя с привилегиями «root» в целевой системе. Уязвимость обусловлена ошибкой в процессе проверки подлинности. 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: данная уязвимость устраняется официальным патчем вендора. в связи со сложившейся обстановкой и введенными санкциями против российской федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	9.8

Ссылки на источники	http://www.dell.com/support/kbdoc/nl-nl/000202365/dsa-2022-216-dell-emc-enterprise-hybrid-cloud-security-update-for-multiple-third-party-component-vulnerabilities (Данный сайт недоступен с IP-адресов Российской Федерации)