НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210922.2 | 22 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в vCenter Server

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	vCenter Server: 6.5, 6.5 U1, 6.5 U3, 6.5 U3a, 6.5 U3b, 6.5 U3c, 6.5 U3d, 6.5 U3e, 6.5 U3f, 6.5 U3g, 6.5 U3h, 6.5 U3i, 6.5 U3j, 6.5 U3k, 6.5 U3l, 6.5 U3m, 6.5 U3n, 6.5 U3o, 6.5 U3p, 6.5.0, 6.5.0a, 6.5.0b, 6.5.0c, 6.5.0d, 6.5u2c, 6.7, 6.7 U3, 6.7 U3a, 6.7 U3b, 6.7 U3c, 6.7 U3d, 6.7 U3e, 6.7 U3f, 6.7 U3g, 6.7 U3h, 6.7 U3i, 6.7 U3k, 6.7 U3l, 6.7 U3m, 6.7 U3n, 6.7.0, 6.7.0d, 7.0, 7.0 U1a, 7.0 U1b, 7.0 U1c, 7.0 U2a, 7.0 U2b
Дата выявления	21 сентября 2021 г.
Дата обновления	21 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-21991	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику получить привилегии администратора в vSphere Client (HTML5) или vCenter Server vSphere Web Client (FLEX / Flash). Уязвимость обусловлена некорректной обработкой токенов сеанса. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/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	8.8

MITRE: CVE-2021-22005	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и запустить вредоносный файл в целевой системе посредством отправки специально сформированных запросов на порт 443/TCP. Уязвимость обусловлена некорректной проверкой файла во время загрузки в сервисе Analytics. 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-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: обновить программное обеспечение	9.8
MITRE: CVE-2021-22006	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к конечным точкам посредством отправки специально сформированных HTTP-запросов на порт 443/TCP. Уязвимость обусловлена некорректной обработкой URI в обратном прокси. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C CWE-285: Некорректная авторизация Рекомендации по устранению: обновить программное обеспечение	8.3
MITRE: CVE-2021-22009	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированных HTTP-запросов на порт 443/TCP. Уязвимость обусловлена некорректным потребление внутренних ресурсов в службе VAPI (vCenter API). CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: обновить программное обеспечение	8.6
MITRE: CVE-2021-22012	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации посредством отправки специально сформированных запросов на порт 443/TCP. Уязвимость обусловлена отсутствием аутентификации в API управления устройством. 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-287: Некорректная аутентификация Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2021-22013	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить атаку с обходом каталогов посредством отправки специально сформированных HTTP-запросов на порт 443/TCP. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов в API управления устройством. 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: обновить программное обеспечение	7.5
MITRE: CVE-2021-22015	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику получить привилегии root в vCenter Server Appliance. Уязвимость обусловлена некорректными разрешениями по умолчанию для файлов и папок, установленных системой. 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-276: Некорректные разрешения, назначаемые по умолчанию Рекомендации по устранению: обновить программное обеспечение	7.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021092118 https://www.vmware.com/security/advisories/VMSA-2021-0020.html