НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201214.4 | 14 декабря 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в продуктах VMware

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware NSX-T VMware Cloud Foundation VMware vCenter Server и VMware ESXi
Дата выявления	20 октября 2020 г.
Дата обновления	10 декабря 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-3992	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного SLP-пакета. Уязвимость обусловлена некоренным использованием освободившейся памяти в службе OpenSLP. 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-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: CVE-2020-3995	Эксплуатация уязвимости позволяет удалённому злоумышленнику с доступом к виртуальной машине выполнить DoS-атаку на гипервизор. Уязвимость обусловлена некоренным управлением памятью в драйвере VMCI. 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-401: Некорректное освобождение памяти до удаления последней ссылки (утечка памяти) Рекомендации по устранению: обновить программное обеспечение.	8.6
MITRE: CVE-2020-3982	Эксплуатация уязвимости позволяет удалённому злоумышленнику с привилегиями администратора на виртуальной машине выполнить произвольный код в гипервизоре посредством запуска специально сформированного файла. Уязвимость обусловлена некорректной проверкой времени использования в устройстве ACPI в рамках реализации команды BDOOR_CMD_PATCH_ACPI_TABLES. CVSSv3.0: AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение.	8.4
MITRE: CVE-2020-3994	Эксплуатация уязвимости позволяет удалённому злоумышленнику, находящемуся между vCenter Server и репозиторием, осуществить атаку «человек по середине», тем самым перехватив сеанс обновления в vCenter Server. Уязвимость обусловлена отсутствием проверки сертификата в vCenter Server. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-295: Некорректная проверка сертификатов Рекомендации по устранению: обновить программное обеспечение.	7.4

Ссылки на источники	https://www.vmware.com/security/advisories/VMSA-2020-0023.html