НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201214.1 | 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 ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Cloud Foundation
Дата выявления	19 ноября 2020 г.
Дата обновления	24 ноября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-4004	Эксплуатация уязвимости позволяет локальному злоумышленнику с привилегиями администратора на виртуальной машине выполнить произвольный код в хостовой системе от имени процесса VMX. Уязвимость обусловлена некоренным использованием освободившейся памяти в USB-контроллере XHCI. CVSSv3.0: AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	9.3

MITRE: CVE-2020-4005	Эксплуатация уязвимости позволяет локальному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректным способом управления определенными системными вызовами. Успешная эксплуатация данной уязвимости возможна только при наличии уязвимости CVE-2020-4004. 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-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://www.vmware.com/security/advisories/VMSA-2020-0026.html