НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200616.5 | 16 июня 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в уязвимости в Intel AMT и ISM

Категория уязвимого продукта	Компоненты рабочих станций и серверных платформ
Уязвимое ПО	Intel (R) AMT и Intel (R) ISM до 11.8.77, 11.12.77, 11.22.77 и 12.0.64, при включённой поддержке удаленного доступа по IPv6.
Дата выявления	9 июня 2020 г.
Дата обновления	12 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-0594	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным и повысить привилегии в целевой системе посредством отправки специально созданного вредоносного IPv6-пакета. Уязвимость обусловлена переполнением буфера в подсистеме IPv6. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: CVE-2020-0595	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным и повысить привилегии в целевой системе посредством отправки специально созданного вредоносного IPv6-пакета. Уязвимость обусловлена ошибкой использования памяти после освобождения в подсистеме IPv6. CVSSv3.1: 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-2020-0596	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в подсистеме DHCPv6. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-200: Разглашение информации Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html http://www.opennet.ru/opennews/art.shtml?num=53149 https://threatpost.com/critical-intel-flaws-fixed-in-active-management-technology/156458/