НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200923.4 | 23 сентября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Xen

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Xen: 3.2, 3.2.0, 3.2.1, 3.2.2, 3.2.3, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.1.0, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.6.1, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.4.0, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.6.0, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.7.0, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.8.0, 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.9.0, 4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.10.0, 4.10.1, 4.10.2, 4.10.3, 4.10.4, 4.11.0, 4.11.1, 4.11.2, 4.11.3, 4.11.4, 4.12.0, 4.12.1, 4.12.2, 4.12.3, 4.13.0, 4.13.1, 4.14.0
Дата выявления	22 сентября 2020 г.
Дата обновления	23 сентября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-25601 CVE-2020-25600 CVE-2020-25603 CVE-2020-25597	Эксплуатация уязвимости позволяет удаленному авторизованному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректным управлением внутренними ресурсами системы программным обеспечением Xen. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C	7.7

CVE-2020-25598 CVE-2020-25604	CWE-399: Уязвимости, связанные с управлением ресурсами CWE-400: Неконтролируемое использование ресурсов (Исчерпание ресурсов) CWE-362: Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (Состояние гонки) Рекомендации по устранению: обновить программное обеспечение.	
MITRE: CVE-2020-25599	Эксплуатация уязвимости позволяет удаленному авторизованному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректной работой функций EVTCHNOP_reset и XEN_DOMCTL_soft_reset. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-362: Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (Состояние гонки) Рекомендации по устранению: обновить программное обеспечение.	9.9
MITRE: CVE-2020-25595	Эксплуатация уязвимости позволяет удаленному авторизованному злоумышленнику повысить привилегии в целевой системе посредством запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректным взаимодействием между программным и аппаратным обеспечением. CVSSv3.0: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-908: Использование неинициализированных ресурсов Рекомендации по устранению: обновить программное обеспечение.	8.5
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020092323	