НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201105.2 | 5 ноября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Synology Router Manager

Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Synology Router Manager (SRM) до v1.2.4-8081
Дата выявления	29 октября 2020 г.
Дата обновления	29 октября 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-27654 CVE-2020-11117	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специальной команды отладки, которая позволяет перезаписывать произвольные файлы. Уязвимость обусловлена некорректной работой службы ldb. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-73: Внешнее управление именем или путем файла Рекомендации по устранению: обновить программное обеспечение.	9.6

MITRE: CVE-2020-27653	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить файлы cookie сеанса в уязвимом приложении посредством выполнения атаки «человек посередине». Уязвимость обусловлена некорректной работой функции HTTP-соединения QuickConnect. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-757: Выбор менее безопасного алгоритма при согласовании (понижение надежности алгоритма) Рекомендации по устранению: обновить программное обеспечение.	8.3
MITRE: CVE-2020-27649	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевому устройству посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной проверкой сертификата в клиенте OpenVPN. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-295: Некорректная проверка сертификатов Рекомендации по устранению: обновить программное обеспечение.	8.3
MITRE: CVE-2020-27651	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевому устройству посредством перехвата файлов cookie сеанса в сетевом трафике. Уязвимость обусловлена отсутствием флага «secure» в файлах cookie сеанса. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-614Отсутствие в HTTPS-сессиях атрибута Secure у конфиденциальных куки-параметров Рекомендации по устранению: обновить программное обеспечение.	8.3

MITRE: CVE-2020-27658	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить файлы cookie сеанса в уязвимом приложении посредством выполнения XSS-атаки. Уязвимость обусловлена отсутствием флага «HttpOnly» в файлах cookie сеанса. 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-1004:Отсутствие флага HttpOnly у конфиденциальных куки-параметров Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1065 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1061 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1058 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1059 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1086