НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210813.1 | 13 августа 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в AT&T Labs Xmill

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Xmill: 0.7
Дата выявления	12 августа 2021 г.
Дата обновления	12 августа 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-21811	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена потерей значимости целых чисел. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-191: Потеря значимости целых чисел (простой или циклический возврат) Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.1

MITRE: CVE-2021-21810	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти в функции HandleFileArg. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.1
MITRE: CVE-2021-21815 CVE-2021-21814 CVE-2021-21813 CVE-2021-21812	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена ошибкой границ памяти в функции HandleFileArg. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	7.8

Ссылки на источники	https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1280 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1279 https://www.cybersecurity-help.cz/vdb/SB2021081202 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1278 https://blog.talosintelligence.com/2021/08/vuln-spotlight-att.html