

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230421.2 | 21 апреля 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Ubuntu

Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Ubuntu: 22.04, 20.04, 18.04, 14.04 vim (Ubuntu package): до 2:8.0.1453-1ubuntu1.13
Дата выявления	19 апреля 2023 г.
Дата обновления	19 апреля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-0351	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	8.4

<p>MITRE: CVE-2022-0361</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-0408</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-121: Переполнение буфера в стеке</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-0443</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>

<p>MITRE: CVE-2022-0554</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику вызвать отказ в обслуживании целевой системы посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-823: Использование для указателя смещения за пределами назначенного диапазона</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-0572</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-0629</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-121: Переполнение буфера в стеке</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>

<p>MITRE: CVE-2022-0685</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-823: Использование для указателя смещения за пределами назначенного диапазона</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-0714</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.4</p>
<p>MITRE: CVE-2022-0729</p>	<p>Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>7.8</p>

MITRE: CVE-2022-2207	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	7.8
-------------------------	--	-----

Ссылки на источники	http://ubuntu.com/security/notices/USN-6026-1
---------------------	---