НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220224.11 | 24 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в Extensis Portfolio

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Extensis Portfolio: 3.0.0 - 3.6.3
Дата выявления	23 февраля 2022 г.
Дата обновления	23 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-24251	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД целевой системе посредством загрузки и запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	9.8

MITRE: CVE-2022-24255	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена наличием жестко заданных учетных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	9.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022022304 http://www.whiteoaksecurity.com/blog/extensis-portfolio-vulnerability-disclosure/