

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230328.1 | 28 марта 2023 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Fraud Risk Management (FRM)

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Fraud Risk Management (FRM): до 14.0.2 Revision 10
Дата выявления	23 марта 2023 г.
Дата обновления	23 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-44228	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H</p> <p>CWE-94: Некорректное управление генерированием кода (внедрение кода)</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>	10.0

<p>MITRE: CVE-2021-45046</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H</p> <p>CWE-94: Некорректное управление генерированием кода (внедрение кода)</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>9.0</p>
<p>MITRE: CVE-2021-4104</p>	<p>Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.</p> <p>CVSSv3.0: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-502: Десериализация недоверенных данных</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>7.5</p>

Ссылки на
источники

http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04230en_us