# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200327.4 | 27 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Множественные уязвимости в Red Hat Fuse

| | |
|---|---|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимое ПО | Red Hat Fuse: 7.0.0, 7.0.1, 7.1.0, 7.1.1, 7.2.0, 7.3.0, 7.3.1, 7.4.0, 7.5.0 |
| Дата выявления | 13 марта 2017 г. |
| Дата обновления | 27 марта 2020 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|---|---|---|
| MITRE:<br>CVE-2019-12384<br>CVE-2017-5929 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса уязвимому приложению. Уязвимость обусловлена некорректной обработкой входных данных классом logback-core.<br><br>CVSS:3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C<br>CWE-502: Десериализация недоверенных данных<br><br>Рекомендации по устранению: Обновить программное обеспечение. | 9.8 |

| | | |
|---|---|---|
| MITRE:<br>CVE-2019-14379 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в модуле SubTypeValidator.java библиотеки Jackson-databind при использовании Ehcache.<br><br>CVSS:3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H/E:U/RL:O/RC:C<br>CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями<br><br>Рекомендации по устранению: Обновить программное обеспечение. | 9.4 |
| MITRE:<br>CVE-2019-17570 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки клиенту XML-RPC специально сформированного пакета через вредоносный сервер XML-RPC. Уязвимость обусловлена некорректной обработкой входных данных методом addResult библиотеки Apache XML-RPC.<br><br>CVSS:3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C<br>CWE-502: Десериализация недоверенных данных<br><br>Рекомендации по устранению: Обновить программное обеспечение. | 8.8 |
| MITRE:<br>CVE-2019-5427 | Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного XML-файла уязвимому приложению. Уязвимость обусловлена некорректной обработкой входных данных классом C3P0ConfigXmlUtils.<br><br>CVSS:3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C<br>CWE-20: Некорректная проверка входных данных<br><br>Рекомендации по устранению: Обновить программное обеспечение. | 7.5 |
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2020032701 | |