

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220124.6 | 24 января 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Oracle WebLogic Server

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Oracle WebLogic Server: до 14.1.1.0.0
Дата выявления	18 января 2022 г.
Дата обновления	18 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-27568 CVE-2022-21371	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	9.1

MITRE: CVE-2021-4104	<p>Эксплуатация уязвимости позволяет 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:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-502: Десериализация недоверенных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.1
MITRE: CVE-2022-21306	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.1

Ссылки на
источники

<http://www.oracle.com/security-alerts/cpujan2022.html#3219>
<https://www.cybersecurity-help.cz/vdb/SB2022011837>