

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201030.11 | 30 октября 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**
Наличие обновления: **ЕСТЬ**

Несанкционированный доступ в продуктах Oracle, использующих библиотеку dom4j

| | |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Идентификатор уязвимости | MITRE: CVE-2020-10683 |
| Идентификатор программной ошибки | CWE-611: Некорректная аутентификация |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому приложению посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена некорректными настройками по умолчанию. |
| Категория уязвимого продукта | Универсальные компоненты и библиотеки Библиотека dom4j до v2.0.3 и v2.1.0 до v2.1.3 Oracle Communications Unified Inventory Management v7.3.0, v7.4.0 Oracle Communications Application Session Controller v3.9m0p1 Oracle Communications Diameter Signaling Router: IDIH v8.0.0-8.2.2 Oracle Banking Platform v2.4.0-2.10.0 Oracle Financial Services Analytical Applications Infrastructure v8.0.6-8.1.0 Oracle Endeca Information Discovery Integrator v3.2.0 Oracle WebCenter Portal v12.2.1.3.0, v12.2.1.4.0 Oracle Health Sciences Empirica Signal v9.0 Oracle Retail Order Broker v15.0, v16.0, v18.0, v19.0, v19.1 Oracle Retail Price Management v14.0.4, v14.1.3.0, v15.0.3.0, v16.0.3.0 Oracle Agile PLM v9.3.3, v9.3.5 Oracle Utilities Framework v2.2.0.0.0, v4.2.0.2.0, v4.2.0.3.0, v4.3.0.1.0 - 4.3.0.6.0, v4.4.0.0.0, v4.4.0.2.0 |
| Уязвимый продукт | Обновить программное обеспечение |
| Рекомендации по устранению | |

| | |
|---------------------------------------------------|-----------------------------------------|
| Дата выявления | 20 октября 2020 г. |
| Дата обновления | 20 октября 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Отсутствует (N) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |
| Влияние на конфиденциальность (C) | Высокое (H) |
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Высокое (H) |
| Степень зрелости доступных средств эксплуатации | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |

<https://nvd.nist.gov/vuln/detail/CVE-2020-10683>
<https://www.oracle.com/security-alerts/cpuoct2020.html?504207>
<https://www.oracle.com/security-alerts/cpuoct2020verbose.html#BGDG>

Ссылки на источники