НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200424.3 | 24 апреля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Oracle Advanced Outbound Telephony

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Oracle Advanced Outbound Telephony до v12.2.9
Дата выявления	22 апреля 2020 г.
Дата обновления	23 апреля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-2857 CVE-2020-2856 CVE-2020-2854 CVE-2020-2871 CVE-2020-2852	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к данным посредством открытия пользователем специально созданного вредоносного веб-сайта или вредоносного документа. Уязвимость обусловлена недостаточной проверкой предоставленных пользователем данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	8.2

MITRE: CVE-2020-2863	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить несанкционированный доступ к данным посредством отправки специально сформированных вредоносных сетевых пакетов. Уязвимость обусловлена недостаточной проверкой предоставленных пользователем данных. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	8.5

Ссылки на источники	https://www.oracle.com/security-alerts/cpuapr2020.html https://www.cybersecurity-help.cz/vdb/SB2020042361