



NCSC-2024-0422

Kwetsbaarheden verholpen in Oracle E-Business Suite

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-10-2024

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Oracle heeft kwetsbaarheden verholpen in E-Business Suite.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om toegang te krijgen tot gevoelige gegevens en deze mogelijk te manipuleren.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2024.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-21206	4.3 MEDIUM
➤ CVE-2024-21250	8.1 HIGH
➤ CVE-2024-21252	8.1 HIGH
➤ CVE-2024-21258	5.3 MEDIUM
➤ CVE-2024-21265	8.1 HIGH
➤ CVE-2024-21266	8.1 HIGH
➤ CVE-2024-21267	8.1 HIGH
➤ CVE-2024-21268	8.1 HIGH
➤ CVE-2024-21269	8.1 HIGH
➤ CVE-2024-21270	8.1 HIGH

> CVE-2024-21271	8.1 HIGH
> CVE-2024-21275	8.1 HIGH
> CVE-2024-21276	8.1 HIGH
> CVE-2024-21277	8.1 HIGH
> CVE-2024-21278	8.1 HIGH
> CVE-2024-21279	8.1 HIGH
> CVE-2024-21280	8.1 HIGH
> CVE-2024-21282	8.1 HIGH

CWE's

CWE	Beschrijving
> CVE-862	Missing Authorization
> CVE-922	Insecure Storage of Sensitive Information
> CVE-863	Incorrect Authorization

Getroffen producten

oracle_corporation
oracle_site_hub
oracle_sourcing
oracle_work_in_process
oracle_advanced_pricing
oracle_applications_manager
oracle_common_applications_calendar
oracle_contract_lifecycle_management_for_public_sector

oracle_cost_management
oracle_enterprise_command_center_framework
oracle_field_service
oracle_financials
oracle_incentive_compensation
oracle_installed_base
oracle_mes_for_process_manufacturing
oracle_process_manufacturing_product_development
oracle_product_hub
oracle_quoting
oracle_service_contracts
oracle
advanced_pricing
applications_manager
common_applications_calendar
contract_lifecycle_management_for_public_sector
cost_management
e-business_suite___12.2.13
e-business_suite___12.2.14
e-business_suite___13
enterprise_command_center_framework
field_service
financials
incentive_compensation

installed_base
mes_for_process_manufacturing
process_manufacturing_product_development
product_hub
quoting
service_contracts
site_hub
sourcing
work_in_process

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.