Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0305

Kwetsbaarheden verholpen in Oracle Siebel CRM

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2024

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

Er zijn kwetsbaarheden verholpen in Oracle Siebel CRM.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Toegang tot gevoelige gegevens
- Toegang tot systeemgegevens
- Manipulatie van gegevens
- (Remote) code execution (Gebruikersrechten)

Oplossingen

Oracle heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Zie de referenties voor meer informatie.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2021-36090
- https://nvd.nist.gov/vuln/detail/CVE-2022-34169
- https://nvd.nist.gov/vuln/detail/CVE-2022-37434
- https://nvd.nist.gov/vuln/detail/CVE-2022-42003
- https://nvd.nist.gov/vuln/detail/CVE-2023-22081
- https://nvd.nist.gov/vuln/detail/CVE-2023-33201
- https://nvd.nist.gov/vuln/detail/CVE-2023-41105
- https://nvd.nist.gov/vuln/detail/CVE-2023-46589
- https://nvd.nist.gov/vuln/detail/CVE-2023-47627
- https://nvd.nist.gov/vuln/detail/CVE-2023-5072
- https://nvd.nist.gov/vuln/detail/CVE-2023-5678
- https://nvd.nist.gov/vuln/detail/CVE-2023-5764
- https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json
- https://www.oracle.com/security-alerts/cpujul2024.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-36090	
CVE-2022-34169	
CVE-2022-37434	
CVE-2022-42003	
CVE-2023-5072	7.5 HIGH
CVE-2023-5678	7.5 HIGH
CVE-2023-5764	7.8 HIGH
CVE-2023-22081	5.3 MEDIUM
CVE-2023-33201	5.3 MEDIUM
CVE-2023-41105	7.5 HIGH
CVE-2023-46589	7.5 HIGH
CVE-2023-47627	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine
CWE-158	Improper Neutralization of Null Byte or NUL Character
CWE-192	Integer Coercion Error
CWE-20	Improper Input Validation
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-295	Improper Certificate Validation
CWE-325	Missing Cryptographic Step

CWE-404	Improper Resource Shutdown or Release
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-502	Deserialization of Untrusted Data
CWE-681	Incorrect Conversion between Numeric Types
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write

Getroffen producten

oracle
siebel_crm_cloud_applications
siebel_crm_deployment
siebel_crm_end_user
siebel_crm_integration
siebel_crm

Disclaimer