Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0026

Kwetsbaarheden verholpen in Oracle JD Edwards

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-01-2025

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 JD Edwards EnterpriseOne Tools (specifiek voor versies prior tot 9.2.9.2).

Duiding

De kwetsbaarheden in Oracle JD Edwards EnterpriseOne Tools stellen ongeauthenticeerde kwaadwillenden in staat om het systeem te compromitteren via HTTP-verzoeken. Dit kan leiden tot ongeautoriseerde toegang tot kritieke gegevens en gegevenswijzigingen.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpujan2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-2976	7.5 HIGH
CVE-2023-3961	9.8 CRITICAL
CVE-2023-4091	9.8 CRITICAL
CVE-2023-4782	7.8 HIGH
CVE-2023-5678	
CVE-2023-6129	6.5 MEDIUM
CVE-2023-38552	8.2 HIGH
CVE-2023-39017	9.8 CRITICAL
CVE-2023-42669	9.8 CRITICAL

CVE-2023-48795	7.5 HIGH
CVE-2024-0727	7.5 HIGH
CVE-2024-21245	5.4 MEDIUM
CVE-2024-22019	8.2 HIGH
CVE-2024-22020	8.2 HIGH
CVE-2024-27280	9.8 CRITICAL
CVE-2024-27281	
CVE-2024-27282	8.1 HIGH
CVE-2024-27983	8.2 HIGH
CVE-2024-29041	6.5 MEDIUM
CVE-2025-21507	5.4 MEDIUM
CVE-2025-21508	6.5 MEDIUM
CVE-2025-21509	6.5 MEDIUM
CVE-2025-21510	7.5 HIGH
CVE-2025-21511	7.5 HIGH
CVE-2025-21512	6.1 MEDIUM
CVE-2025-21513	6.1 MEDIUM
CVE-2025-21514	5.3 MEDIUM
CVE-2025-21515	8.8 HIGH
CVE-2025-21517	4.3 MEDIUM
CVE-2025-21524	9.8 CRITICAL
CVE-2025-21527	6.1 MEDIUM
CVE-2025-21538	6.1 MEDIUM

CVE-2025-21552	**6.5 MEDIUM**

CWE's

CWE	Beschrijving
CWE-222	Truncation of Security-relevant Information
CWE-328	Use of Weak Hash
CWE-126	Buffer Over-read
CWE-379	Creation of Temporary File in Directory with Insecure Permissions
CWE-440	Expected Behavior Violation
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-354	Improper Validation of Integrity Check Value
CWE-552	Files or Directories Accessible to External Parties
CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-400	Uncontrolled Resource Consumption
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-787	Out-of-bounds Write
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-606	Unchecked Input for Loop Condition
CWE-1322	Use of Blocking Code in Single-threaded, Non-blocking Context
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-325	Missing Cryptographic Step

CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-476	NULL Pointer Dereference
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-502	Deserialization of Untrusted Data
CWE-122	Heap-based Buffer Overflow
CWE-20	Improper Input Validation
CWE-276	Incorrect Default Permissions

Getroffen producten

oracle
jd_edwards_enterpriseone_orchestrator
jd_edwards_enterpriseone_tools
jd_edwards_world_security

Disclaimer