

CVE-2022-21445

Oracle ADF Faces Deserialization of Untrusted Data Vulnerability

CISA KEV since Sep 18, 2024

Actively exploited

Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in takeover of Oracle Application Development Framework (ADF).

EVRS 77/100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.625 99.19th percentile · FIRST	CISA DEADLINE Oct 9, 2024 KEV since 2024 · listed over a year
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.625 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Note: Oracle Application Development Framework (ADF) is downloaded via Oracle JDeveloper Product. Please refer to Fusion Middleware Patch Advisor for more details. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
application development framework	12.2.1.3.0 12.2.1.4.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-7f3x-fvqf-q6q5
NVD nvd.nist.gov/vuln/detail/CVE-2022-21445

Additional guidance oracle.com/security-alerts/cpuapr2022.html
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-26669

Current data evulnable.com/vulnerability-management/cve/CVE-2022-21445

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.