TLP: WHITE

Advisory Alert

Alert Number: **AAA20250725** **Date:** **July 25, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Unauthenticated Remote Code Execution Vulnerabilities
Oracle	**High**	Security Update
SUSE	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Unauthenticated Remote Code Execution Vulnerabilities (CVE-2025-20281, CVE-2025-20282, CVE-2025-20337)
Description	Cisco has released security updates addressing multiple Unauthenticated Remote Code Execution that exist in Cisco Identity Services Engine. **CVE-2025-20281** and **CVE-2025-20337** - Multiple vulnerabilities in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit these vulnerabilities. **CVE-2025-20282** - A vulnerability in an internal API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to upload arbitrary files to an affected device and then execute those files on the underlying operating system as root. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE and ISE-PIC Release 3.3 and 3.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

Affected Product	**Oracle**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-30751)
Description	Oracle has released security updates addressing a vulnerability that exists in Oracle Database. This vulnerability could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Database versions 19.27 and 23.4 - 23.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujul2025.html

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22115, CVE-2022-49465, CVE-2024-53146, CVE-2024-53173, CVE-2024-53214, CVE-2024-57893, CVE-2025-21772)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6, 12-SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6, 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6, 12 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502514-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502507-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21587, CVE-2025-30698, CVE-2025-2900, CVE-2025-4447)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 Query Management Facility. These vulnerabilities could be exploited by malicious users to cause Denial of Service, confidentiality and integrity impacts. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Db2 Query Management Facility version 13.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7240530

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.