Advisory Alert

Alert Number: **AAA20241119** **Date:** **November 19, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**Critical**	Authentication Bypass Vulnerability
Oracle	**High**	Security Update
IBM	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**	Privilege Escalation Vulnerability

Description

Affected Product	**Palo Alto**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-0012)
Description	Palo Alto has released security updates addressing an Authentication Bypass Vulnerability that exists in their products. **CVE-2024-0012-** An authentication bypass vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 Versions before 11.2.4-h1 PAN-OS 11.1 Versions before 11.1.5-h1 PAN-OS 11.0 Versions before 11.0.6-h1 PAN-OS 10.2 Versions before 10.2.12-h2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-0012

Affected Product	**Oracle**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-21287)
Description	Oracle has released security updates addressing a vulnerability that exists in Oracle Agile PLM Framework. **CVE-2024-21287 -** A vulnerability exists in the Oracle Agile PLM Framework, part of the Oracle Supply Chain product suite. This vulnerability allows an unauthenticated attacker with network access via HTTP to compromise the Oracle Agile PLM Framework. Successful exploitation of this vulnerability could result in unauthorized access to sensitive data or full access to all data accessible through the Oracle Agile PLM Framework. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Agile PLM Framework, version 9.3.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/alert-cve-2024-21287.html

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45071, CVE-2024-45085, CVE-2024-45073, CVE-2024-7254, CVE-2024-45072)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7176401 • https://www.ibm.com/support/pages/node/7176392 • https://www.ibm.com/support/pages/node/7176394 • https://www.ibm.com/support/pages/node/7176396 • https://www.ibm.com/support/pages/node/7176403

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26671, CVE-2022-48796, CVE-2024-46858)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:9943 • https://access.redhat.com/errata/RHSA-2024:9942

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-9474)
Description	Palo Alto has released security updates addressing a privilege escalation vulnerability in PAN-OS software that allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 versions before 11.2.4-h1 PAN-OS 11.1 versions before 11.1.5-h1 PAN-OS 11.0 versions before 11.0.6-h1 PAN-OS 10.2 versions before 10.2.12-h2 PAN-OS 10.1 versions before 10.1.14-h6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-9474

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.