Advisory Alert

Alert Number: AAA20250224 **Date:** February 24, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Palo Alto	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-13936,CVE-2021-42392,CVE-2021-44228,CVE-2021-44906,CVE-2021-45046,CVE-2022-1471,CVE-2022-41881,CVE-2022-42003,CVE-2022-42004,CVE-2022-42889,CVE-2022-45047,CVE-2022-45693,CVE-2022-46363,CVE-2020-8840,CVE-2020-9546,CVE-2020-9547,CVE-2020-9548,CVE-2020-10672,CVE-2020-10673,CVE-2021-3717)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Arbitrary Code Execution, Denial Of Service, and Remote Code Execution. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.3 EUS 7.3 x86_64 JBoss Enterprise Application Platform 7.1 EUS 7.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:1747 • https://access.redhat.com/errata/RHSA-2025:1746

Affected Product	**Palo Alto**
Severity	**High**, **Medium** - Initial release date **February 13, 2025 (AAA20250213)**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-5921, CVE-2025-0109, CVE-2025-0111, CVE-2025-0108)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Unauthenticated File Deletion, Authenticated File Read, Authentication Bypass and Privilege Escalation. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect App 6.1 All on Windows GlobalProtect App 6.1 All on macOS GlobalProtect App 6.1 All on Linux GlobalProtect App 6.2 Versions Prior to 6.2.6* on Windows GlobalProtect App 6.2 Versions Prior to 6.2.6-c857* on macOS GlobalProtect App 6.2 Versions Prior to 6.2.1-c31* on Linux GlobalProtect App 6.3 Versions Prior to 6.3.2* on Windows GlobalProtect App 6.3 Versions Prior to 6.3.2* on macOS PAN-OS 10.1 Versions Prior to 10.1.14-h9 PAN-OS 10.2 Versions Prior to 10.2.7-h24 PAN-OS 10.2 Versions Prior to 10.2.8-h21 PAN-OS 10.2 Versions Prior to 10.2.9-h21 PAN-OS 10.2 Versions Prior to 10.2.10-h14 PAN-OS 10.2 Versions Prior to 10.2.11-h12 PAN-OS 10.2 Versions Prior to 10.2.12-h6 PAN-OS 10.2 Versions Prior to 10.2.13-h3 PAN-OS 11.1 Versions Prior to 11.1.2-h18 PAN-OS 11.1 Versions Prior to 11.1.4-h13 PAN-OS 11.1 Versions Prior to 11.1.6-h1 PAN-OS 11.2 Versions Prior to 11.2.4-h4 PAN-OS 11.2 Versions Prior to 11.2.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-5921 • https://security.paloaltonetworks.com/CVE-2025-0109 • https://security.paloaltonetworks.com/CVE-2025-0111 • https://security.paloaltonetworks.com/CVE-2025-0108

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.