Severity

Medium

Analysis Summary

CVE-2022-0025 CVSS:6.7

Palo Alto Networks Cortex XDR Agent could allow a local authenticated attacker to gain elevated privileges on the system, caused by an uncontrolled search path element flaw. By using a specially-crafted file, an authenticated attacker could exploit this vulnerability to execute arbitrary programs with elevated privileges.

CVE-2022-0024 CVSS:7.2

Palo Alto Networks PAN-OS could allow a remote authenticated attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious configuration file, which could allow the attacker to execute arbitrary code with root privileges on the system.

Impact

- Privilege Escalation
- Unauthorized Access

Indicators Of Compromise

CVE

- CVE-2022-0025
- CVE-2022-0024

Affected Vendors

Palo Alto

Affected Products

- Palo Alto Networks Cortex XDR Agent 7.7
- Palo Alto Networks PAN-OS 9.0.0
- Palo Alto Networks PAN-OS 8.1
- Palo Alto Networks PAN-OS 9.1.0

Remediation

Refer to Palo Alto Networks Security Advisories for patch, upgrade or suggested workaround information.

CVE-2022-0025 CVE-2022-0024