Severity

Medium

Analysis Summary

CVE-2022-0026 CVSS:7.2

Palo Alto Networks Cortex XDR Agent could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper ownership management. By sending a specially-crafted request, an authenticated attacker could exploit this vulnerability to execute arbitrary program with elevated privileges.

CVE-2022-0027 CVSS:4.3

Palo Alto Networks Cortex XSOAR could allow a remote authenticated attacker to obtain sensitive information, caused by improper authorization validation. By generating an email report, an attacker could exploit this vulnerability to obtain summary information about all incidents in the Cortex XSOAR instance, and use this information to launch further attacks against the affected system.

Impact

- Privilege Escalation
- Information Disclosure

Indicators Of Compromise

CVE

CVE-2022-0026

CVE-2022-0027

Affected Vendors

Palo Alto

Affected Products

- Palo Alto Networks Cortex XDR Agent 6.1
- Palo Alto Networks Cortex XDR Agent 7.7
- Palo Alto Networks Cortex XDR Agent 7.6
- Palo Alto Networks Cortex XDR Agent 7.5 CE
- Palo Alto Networks Cortex XSOAR 6.1.0
- Palo Alto Networks Cortex XSOAR 6.2.0
- Palo Alto Networks Cortex XSOAR 6.5.0
- Palo Alto Networks Cortex XSOAR 6.6.0

Remediation

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

CVE-2022-0026 CVE-2022-0027