Severity

Medium

Analysis Summary

CVE-2022-29616 CVSS:5.3

SAP Host Agent and NetWeaver and ABAP Platform are vulnerable to a denial of service, caused by a memory corruption. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service condition.

CVE-2022-28774 CVSS:5.3

SAP Host Agent could allow a local authenticated attacker to obtain sensitive information, caused by the storage of restricted information in the log files. By gaining access to the log files, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-29611 CVSS:6.5

SAP NetWeaver Application Server for ABAP and ABAP Platform could allow a remote authenticated attacker to gain elevated privileges on the system, caused by improper authorization validation. By sending a specially-crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

CVE-2022-29610 CVSS:5.4

SAP NetWeaver Application Server ABAP is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote authenticated attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim’s Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim’s cookie-based authentication credentials.

Impact

- Denial of Service
- Information Disclosure
- Cross-Site Scripting

Indicators Of Compromise

CVE

- CVE-2022-29616
- CVE-2022-28774
- CVE-2022-29611
- CVE-2022-29610

Affected Vendors

SAP

Affected Products

- SAP NetWeaver ABAP Platform 7.40
- SAP NetWeaver ABAP Platform KRNL64NUC 7.22
- SAP NetWeaver ABAP Platform KRNL64NUC 7.22EXT

- SAP NetWeaver ABAP Platform KRNL64NUC 7.49
- SAP Host Agent 7.22
- SAP NetWeaver AS for ABAP 731
- SAP NetWeaver AS for ABAP 740
- SAP NetWeaver AS for ABAP 750
- SAP NetWeaver AS for ABAP 700
- SAP NetWeaver Application Server ABAP 753
- SAP NetWeaver Application Server ABAP 754
- SAP NetWeaver Application Server ABAP 755
- SAP NetWeaver Application Server ABAP 756

Remediation

Current SAP customers should refer to SAP note for patch information, available from the SAP Web site (login required).

CVE-2022-29616 CVE-2022-28774 CVE-2022-29611 CVE-2022-29610