

Severity

Medium

Analysis Summary

CVE-2022-29613

SAP Employee Self Service could allow a remote authenticated attacker to obtain sensitive information, caused by improper input validation. By gaining access to the Sysmon event logs, an attacker could exploit this vulnerability to obtain personal information of other users, and use this information to launch further attacks against the affected system.

Impact

- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-29613

Affected Vendors

SAP

Affected Products

- SAP Employee Self Service 605

Remediation

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