Severity

Medium

Analysis Summary

CVE-2022-27667 CVSS:5.3

SAP BusinessObjects Business Intelligence Platform could allow a remote attacker to obtain sensitive information, caused by improper access control. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-27657 CVSS:2.7

SAP Focused Run could allow a remote authenticated attacker to traverse directories on the system, caused by improper validation of user request. An attacker could send a specially-crafted URL request containing “dot dot” sequences (/../) to view arbitrary files on the system.

CVE-2022-27654 CVSS:6.5

SAP 3D Visual Enterprise Viewer is vulnerable to a denial of service, caused by a improper input validation. By persuading a victim to open a specially-crafted Photoshop Document file, a remote attacker could exploit this vulnerability to cause the application to crash.

CVE-2022-27655 CVSS:7.6

SAP 3D Visual Enterprise Viewer is vulnerable to a denial of service, caused by a improper input validation. By persuading a victim to open a specially-crafted Universal 3D file, a remote attacker could exploit this vulnerability to cause the application to crash.

CVE-2022-26109 CVSS:6.5

SAP 3D Visual Enterprise Viewer is vulnerable to a denial of service, caused by a improper input validation. By persuading a victim to open a specially-crafted Portable Document Format file, a remote attacker could exploit this vulnerability to cause the application to crash.

CVE-2022-26108 CVSS:6.5

SAP 3D Visual Enterprise Viewer is vulnerable to a denial of service, caused by a improper input validation. By persuading a victim to open a specially-crafted Picture Exchange file, a remote attacker could exploit this vulnerability to cause the application to crash.

CVE-2022-26107 CVSS:7.6

SAP 3D Visual Enterprise Viewer is vulnerable to a denial of service, caused by a improper input validation. By persuading a victim to open a specially-crafted Jupiter Tesselation file, a remote attacker could exploit this vulnerability to cause the application to crash.

CVE-2022-26106 CVSS:6.5

SAP 3D Visual Enterprise Viewer is vulnerable to a denial of service, caused by a improper input validation. By persuading a victim to open a specially-crafted Computer Graphics Metafile file, a remote attacker could exploit this vulnerability to cause the application to crash.

CVE-2022-26105 CVSS:6.1

SAP NetWeaver Enterprise Portal is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim’s Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim’s cookie-based authentication credentials.

Impact

- Information Disclosure

- Denial of Service
- Cross-Site scripting

Indicator Of Compromise

CVE

- CVE-2022-27667
- CVE-2022-27657
- CVE-2022-27654
- CVE-2022-27655
- CVE-2022-26109
- CVE-2022-26108
- CVE-2022-26107
- CVE-2022-26106
- CVE-2022-26105

Affected Vendors

SAP

Affected Products

- SAP BusinessObjects Business Intelligence Platform 430
- SAP Focused Run 1.0
- SAP 3D Visual Enterprise Viewer 9.0
- SAP NetWeaver Enterprise Portal 7.11
- SAP NetWeaver Enterprise Portal 7.20
- SAP NetWeaver Enterprise Portal 7.30
- SAP NetWeaver Enterprise Portal 7.31

Remediation

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

SAP BusinessObjects Business

SAP Focused Run

SAP 3D Visual Enterprise

SAP NetWeaver Enterprise