



CVE-2022-35168

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-35168 |
| State | PUBLIC |
| Assigner | cna@sap.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-07-12 21:15:00 UTC |
| Updated | 2022-07-20 18:09:00 UTC |
| Description | Due to improper input sanitization of XML input in SAP Business One - version 10.0, an attacker can perform a denial-of-se |

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|--------------|---------|--------|---------|----------|
| Application | Sap | Business One | 10.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|---------------------------|---------|---|---------------------|
| launchpad.support.sap.com | MISC | launchpad.support.sap.com | |
| Access Denied | MISC | www.sap.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report