



# CVE-2022-35295

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

## Summary

<b>CVE</b>	CVE-2022-35295
<b>State</b>	PUBLIC
<b>Assigner</b>	cna@sap.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-13 16:15:00 UTC
<b>Updated</b>	2023-03-01 16:34:00 UTC
<b>Description</b>	In SAP Host Agent (SAPOSCOL) - version 7.22, an attacker may use files created by saposcol to escalate privileges for the

## Risk And Classification

**Problem Types:** CWE-755

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Businessobjects Business Intelligence Platform	420	All	All	All
Application	Sap	Businessobjects Business Intelligence Platform	430	All	All	All
Application	Sap	Host Agent	7.22	All	All	All

## References

### Reference

[launchpad.support.sap.com](https://launchpad.support.sap.com)

Full Disclosure: SEC Consult SA-20221213-0 :: Privilege Escalation Vulnerabilities (UNIX Insecure File Handling) in SAP Host Agent (saposcol)

Improper error handling in CLA assistant can cause crash · Advisory · cla-assistant/cla-assistant · GitHub

Access Denied

SAP@ Host Agent Privilege Escalation ≈ Packet Storm

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)