



CVE-2014-8587

Published on: 11/04/2014 12:00:00 AM UTC

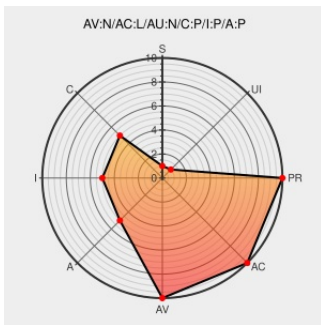
Last Modified on: 03/23/2021 11:25:52 PM UTC

CVE-2014-8587

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Commoncryptolib](#) from [Sap](#) contain the following vulnerability:

SAPCRYPTOLIB before 5.555.38, SAPSECULIB, and CommonCryptoLib before 8.4.30, as used in SAP NetWeaver AS for ABAP and SAP HANA, allows remote attackers to spoof Digital Signature Algorithm (DSA) signatures via unspecified vectors.

CVE-2014-8587 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | LOW | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| PARTIAL | PARTIAL | PARTIAL |

CVE References

| Description | Tags | Link |
|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Security Advisory SA57606 - SAP HANA / NetWeaver Application Server ABAP Digital Signature Spoofing Vulnerability - Secunia | web.archive.org text/html | SECUNIA 57606 |
| No Description Provided | service.sap.com text/html | CONFIRM service.sap.com/sap/support/notes/2067859 |
| JavaScript is not available. | nitter.domain.glass text/html | CONFIRM twitter.com/SAP_Gsupport/status/522401681997570048 |
| SAP Security Note 2067859 Potential Exposure to Digital Signature Spoofing Onapsis | web.archive.org text/html Inactive Link Not Archived | MISC blog.onapsis.com/sap-security-note-2067859-potential-exposure-to-digital-signature-spoofing/ |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further.

are more appropriate for your purposes. CVEreport does not necessarily endorse the views expressed, or content, that are linked from these sites. CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------|---------------------------------|---------|--------|---------|----------|
| Application | Sap | Commoncryptolib | All | All | All | All |
| Application | Sap | Hana | - | All | All | All |
| Application | Sap | Hana | - | All | All | All |
| Application | Sap | Netweaver | All | All | All | All |
| Application | Sap | Netweaver | All | All | All | All |
| Application | Sap | Sapcryptolib | All | All | All | All |
| Application | Sap | Sapseculib | - | All | All | All |
| Application | Sap | Sapseculib | - | All | All | All |

cpe:2.3:a:sap:commoncryptolib:*:*:*:*:*:*:

cpe:2.3:a:sap:hana:-:*:*:*:*:*:

cpe:2.3:a:sap:hana:-:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:*:*:*:*:*:*:

cpe:2.3:a:sap:sapcryptolib:*:*:*:*:*:*:

cpe:2.3:a:sap:sapseculib:-:*:*:*:*:*:

cpe:2.3:a:sap:sapseculib:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)