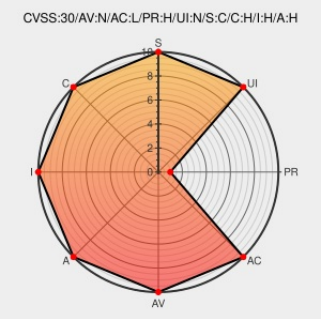
CVE-2016-7435

Published on: 10/05/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

CVE-2016-7435

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Netweaver from Sap contain the following vulnerability:

The (1) SCTC_REFRESH_EXPORT_TAB_COMP, (2) SCTC_REFRESH_CHECK_ENV, and (3) SCTC_TMS_MAINTAIN_ALOG functions in the SCTC subpackage in SAP Netweaver 7.40 SP 12 allow remote authenticated users with certain permissions to execute arbitrary commands via vectors involving a CALL 'SYSTEM' statement, aka SAP Security Note 2260344.

CVE-2016-7435 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Full Disclosure: Onapsis Security Advisory ONAPSIS-2016-043: SAP OS Command Injection in	Mailing List Third Party Advisory	FULLDISC 20161003 Onapsis Security Advisory ONAPSIS-2016-043: SAP OS Command Injection in

SCTC_TMS_MAINTAIN_ALOG	seclists.org text/html	SCTC_TMS_MAINTAIN_ALOG
Full Disclosure: Onapsis Security Advisory ONAPSIS-2016-041: SAP OS Command Injection in SCTC_REFRESH_EXPORT_TAB_COMP	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20161003 Onapsis Security Advisory ONAPSIS-2016-041: SAP OS Command Injection in SCTC_REFRESH_EXPORT_TAB_COMP
SAP OS Command Injection in SCTC_REFRESH_EXPORT_TAB_COMP | Onapsis	Third Party Advisory www.onapsis.com text/html	MISC www.onapsis.com/research/security-advisories/sap-os-command-injection-sctcrefreshexporttabcomp
SAP OS Command Injection in SCTC_TMS_MAINTAIN_ALOG | Onapsis	Third Party Advisory www.onapsis.com text/html	MISC www.onapsis.com/research/security-advisories/sap-os-command-injection-sctctmsmaintainalog
SAP Netweaver CVE-2016-7435 Multiple OS Command Injection Vulnerabilities	cve.report (archive) text/html	BID 93272
Full Disclosure: Onapsis Security Advisory ONAPSIS-2016-042: SAP OS Command Injection in SCTC_REFRESH_CHECK_ENV	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20161003 Onapsis Security Advisory ONAPSIS-2016-042: SAP OS Command Injection in SCTC_REFRESH_CHECK_ENV
SAP OS Command Injection in SCTC_REFRESH_CHECK_ENV | Onapsis	Third Party Advisory www.onapsis.com text/html	MISC www.onapsis.com/research/security-advisories/sap-os-command-injection-sctcrefreshcheckenv
Analyzing SAP Security Notes March 2016 | Onapsis	Third Party Advisory www.onapsis.com text/html	MISC www.onapsis.com/blog/analyzing-sap-security-notes-march-2016

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver	7.40	sp12	All	All
Application	Sap	Netweaver	7.40	sp12	All	All

cpe:2.3:a:sap:netweaver:7.40:sp12:*:*:*:*:*:*:

cpe:2.3:a:sap:netweaver:7.40:sp12:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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