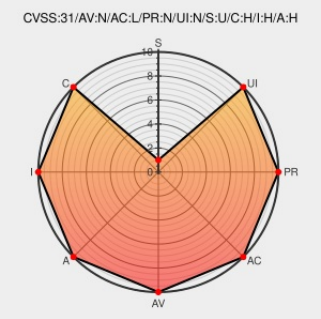
CVE-2018-11741

Published on: 12/26/2018 12:00:00 AM UTC

Last Modified on: 09/13/2021 11:13:00 AM UTC

CVE-2018-11741

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



Certain versions of Univerge Sv9100 Webpro from Nec contain the following vulnerability:

NEC Univerge Sv9100 WebPro 6.00.00 devices have Predictable Session IDs that result in Account Information Disclosure via Home.htm?sessionId=#####&GOTO(8) URIs.

CVE-2018-11741 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Full Disclosure: CVE-2018-11741 / CVE-2018-11742 / NEC Univerge Sv9100 WebPro - 6.00 / Predictable Session ID / Clear Text Password Storage	Exploit, Mailing List, Third Party Advisory, seclists.org, text/html	FULLDISC 20181204 CVE-2018-11741 / CVE-2018-11742 / NEC Univerge Sv9100 WebPro - 6.00 / Predictable Session ID / Clear Text Password Storage

	Exploit Third Party Advisory hyp3rlinx.altervista.org text/plain	MISC hyp3rlinx.altervista.org/advisories/NEC-UNIVERGE-WEBPRO-v6.00-PREDICTABLE-SESSIONID-CLEARTEXT-PASSWORDS.txt
NEC Univerge Sv9100 WebPro - 6.00 - Predictable Session ID / Clear Text Password Storage - Hardware webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 45942
NEC Univerge Sv9100 WebPro 6.00.00 Predictable Session ID / Cleartext Passwords ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/150610/NEC-Univerge-Sv9100-WebPro-6.00.00-Predictable-Session-ID-Cleartext-Passwords.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nec	Univerge Sv9100 Webpro	-	All	All	All
Operating System	Nec	Univerge Sv9100 Webpro Firmware	6.00.00	All	All	All
Hardware	Necom	Univerge Sv9100 Webpro	-	All	All	All
Hardware	Necom	Univerge Sv9100 Webpro	-	All	All	All
Operating System	Necom	Univerge Sv9100 Webpro Firmware	6.00.00	All	All	All
Operating System	Necom	Univerge Sv9100 Webpro Firmware	6.00.00	All	All	All

cpe:2.3:h:nec:univerge_sv9100_webpro:-:*:*:*:*:*:*:*:

cpe:2.3:o:nec:univerge_sv9100_webpro_firmware:6.00.00:*:*:*:*:*:*:*:

cpe:2.3:h:necom:univerge_sv9100_webpro:-:*:*:*:*:*:*:*:

cpe:2.3:h:necom:univerge_sv9100_webpro:-:*:*:*:*:*:*:*:

cpe:2.3:o:necom:univerge_sv9100_webpro_firmware:6.00.00:*:*:*:*:*:*:*:

cpe:2.3:o:necom:univerge_sv9100_webpro_firmware:6.00.00:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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