



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](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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 [M](#) 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

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, 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
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

© [CVE.report](#) 2023   |

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](#)