



CVE-2013-7282

Published on: 01/10/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7282

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ns-wir150ne](#) from [Nisuta](#) contain the following vulnerability:

The management web interface on the Nisuta NS-WIR150NE router with firmware 5.07.41 and Nisuta NS-WIR300N router with firmware 5.07.36_NIS01 allows remote attackers to bypass authentication via a "Cookie: :language=en" HTTP header.

CVE-2013-7282 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Nisuta NS-WIR150NE, NS-WIR300N Wireless Routers Remote Management Web Interface Authentication Bypass Vulnerability

[Exploit](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[MISC](#) www.ampliasecurity.com/advisories/nisuta-nswir150ne-nswir300n-wireless-router-remote-management-web-interface-authentication-bypass-vulnerability.html

[Exploit](#)
[www.ampliasecurity.com](#)
[text/x-c](#)
[Inactive Link](#) [Not Archived](#)

[MISC](#) www.ampliasecurity.com/advisories/AMPLIA-ARA050913.txt

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 	Nisuta	Ns-wir150ne	-	All	All	All
Hardware 	Nisuta	Ns-wir150ne	-	All	All	All
Operating System	Nisuta	Ns-wir150ne Firmware	5.07.41	All	All	All
Operating System	Nisuta	Ns-wir150ne Firmware	5.07.41	All	All	All
Hardware 	Nisuta	Ns-wir300n	-	All	All	All
Hardware 	Nisuta	Ns-wir300n	-	All	All	All
Operating System	Nisuta	Ns-wir300n Firmware	5.07.36_nis01	All	All	All
Operating System	Nisuta	Ns-wir300n Firmware	5.07.36_nis01	All	All	All
cpe:2.3:h:nisuta:ns-wir150ne:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:nisuta:ns-wir150ne:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:nisuta:ns-wir150ne_firmware:5.07.41:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:nisuta:ns-wir150ne_firmware:5.07.41:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:nisuta:ns-wir300n:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:nisuta:ns-wir300n:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:nisuta:ns-wir300n_firmware:5.07.36_nis01:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:nisuta:ns-wir300n_firmware:5.07.36_nis01:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)