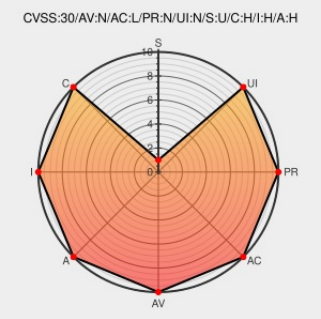
CVE-2019-9161

Published on: 04/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:08 PM UTC

CVE-2019-9161

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



Certain versions of Sundray Wan Controller from Xinruidz contain the following vulnerability:

WAC on the Sangfor Sundray WLAN Controller version 3.7.4.2 and earlier has a Remote Code Execution issue allowing remote attackers to achieve full access to the system, because shell metacharacters in the nginx_webconsole.php Cookie header can be used to read an etc/config/wac/wns_cfg_admin_detail.xml file containing the admin password. (The password for root is the WebUI admin password concatenated with a static string.)

CVE-2019-9161 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: 10 - HIGH

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

CVE References

Description	Tags	Link
国家信息安全漏洞共享平台	Third Party Advisory	MISC www.cnvd.org.cn/flaw/show/CNVD-2019-07679

国家信息安全漏洞共享平台 | Third Party Advisory | MISC www.cnvd.org.cn/flaw/show/CNVD-2019-07679
web.archive.org
text/html
Inactive Link | Not Archived

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	Xinruidz	Sundray Wan Controller	-	All	All	All
Hardware	Xinruidz	Sundray Wan Controller	-	All	All	All
Operating System	Xinruidz	Sundray Wan Controller Firmware	All	All	All	All

cpe:2.3:h:xinruidz:sundray_wan_controller:-:*:*:*:*:*:*:*:

cpe:2.3:h:xinruidz:sundray_wan_controller:-:*:*:*:*:*:*:*:

cpe:2.3:o:xinruidz:sundray_wan_controller_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID | Next ID→