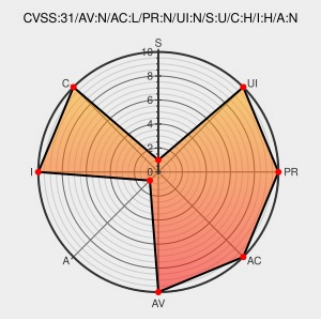
CVE-2019-12510

Published on: 02/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12510

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



Certain versions of Nighthawk X10-r9000 from Netgear contain the following vulnerability:

In NETGEAR Nighthawk X10-R900 prior to 1.0.4.26, an attacker may bypass all authentication checks on the device's "NETGEAR Genie" SOAP API ("/soap/server_sa") by supplying a malicious X-Forwarded-For header of the device's LAN IP address (192.168.1.1) in every request. As a result, an attacker may modify almost all of the device's settings and view various configuration settings.

CVE-2019-12510 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	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
SOHOpelessly Broken 2.0 - Independent Security Evaluators	Exploit, Third Party Advisory	MISC www.ise.io/casestudies/sohopelessly-broken-2-0/

www.ise.io
text/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	Netgear	Nighthawk X10-r9000	-	All	All	All
Hardware	Netgear	Nighthawk X10-r9000	-	All	All	All
Operating System	Netgear	Nighthawk X10-r9000 Firmware	All	All	All	All
Operating System	Netgear	Nighthawk X10-r9000 Firmware	All	All	All	All

cpe:2.3:h:netgear:nighthawk_x10-r9000:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:nighthawk_x10-r9000:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:nighthawk_x10-r9000_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:nighthawk_x10-r9000_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→