



CVE-2019-12511

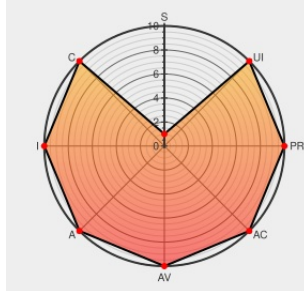
Published on: 02/24/2020 12:00:00 AM UTC

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

CVE-2019-12511

[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 [Nighthawk X10-r9000](#) from [Netgear](#) contain the following vulnerability:

In NETGEAR Nighthawk X10-R9000 prior to 1.0.4.26, an attacker may execute arbitrary system commands as root by sending a specially-crafted MAC address to the "NETGEAR Genie" SOAP endpoint at AdvancedQoS:GetCurrentBandwidthByMAC. Although this requires QoS being enabled, advanced QoS being enabled, and a valid

authentication JWT, additional vulnerabilities (CVE-2019-12510) allow an attacker to interact with the entire SOAP API without authentication. Additionally, DNS rebinding techniques may be used to exploit this vulnerability remotely. Exploiting this vulnerability is somewhat involved. The following limitations apply to the payload and must be overcome for successful exploitation: - No more than 17 characters may be used. - At least one colon must be included to prevent mangling. - A single-quote and meta-character must be used to break out of the existing command. - Parent command remnants after the injection point must be dealt with. - The payload must be in all-caps. Despite these limitations, it is still possible to gain access to an interactive root shell via this vulnerability. Since the web server assigns certain HTTP headers to environment variables with all-caps names, it is possible to insert a payload into one such header and reference the subsequent environment variable in the injection point.

CVE-2019-12511 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: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

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

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

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](#)