Check If Your Netgear Router is also Vulnerable to this Password Bypass Flaw

---

Posted by Hermes 02/19/2017

Again bad news for consumers with Netgear routers: Netgear routers hit by another serious security vulnerability, but this time more than two dozens router models are affected.

Security researchers from Trustwave are warning of a new authentication vulnerability in at least 31 models of Netgear models that potentially affects over one million Netgear customers.

The new vulnerability, discovered by Trustwave's SpiderLabs researcher Simon Kenin, can allow remote hackers to obtain the admin password for the Netgear router through a flaw in the password recovery process.

Kenin discovered the flaw (CVE-2017-5521) when he was trying to access the management page of his Netgear router but had forgotten its password.

Exploiting the Bug to Take Full Access on Affected Routers

So, the researcher started looking for ways to hack his own router and found a couple of exploits from 2014 that he leveraged to discover this flaw which allowed him to query routers and retrieve their login credentials easily, giving him full access to the device.

But Kenin said the newly discovered flaw could be remotely exploited only if the router's remote management option is enabled.

While the router vendor claims the remote management option is turned off on its routers by default, according to the researcher, there are "hundreds of thousands, if not over a million" routers left remotely accessible.

"The vulnerability can be used by a remote attacker if remote administration is set to be internet facing. By default this is not turned on," Kenin said. "However, anyone with physical access to a network with a vulnerable router can exploit it locally. This would include public Wi-Fi spaces like cafés and libraries using the vulnerable equipment."

If exploited by bad actors, the vulnerability that completely bypasses any password on a Netgear router could give hackers complete control of the affected router, including the ability to change its configuration, turn it into botnets or even upload entirely new firmware.

After trying out his flaw on a range of Netgear routers, Kenin was surprised to know that more than ten thousand vulnerable devices used the flawed firmware and can be accessed remotely.

He has also released an exploit code for testing purpose, written in Python.

List of Vulnerable NETGEAR Router Models

The SpiderLabs researcher stressed that the vulnerability is very serious as it affects a large number of Netgear router models. Here's a list of affected Netgear routers:

- R8500
- R8300
- R7000
- R6400
- R7300DST
- R7100LG
- R6300v2
- WNDR3400v3
- WNR3500Lv2
- R6250
- R6700
- R6900
- R8000
- R7900
- WNDR4500v2
- R6200v2
- WNDR3400v2
- D6220
- D6400
- C6300 (firmware released to ISPs)

Update the Firmware of your NETGEAR Router Now!

Kenin notified Netgear of the flaw, and the company confirmed the issue affects a large number of its products.

Netgear has released firmware updates for all of its affected routers, and users are strongly advised to upgrade their devices.

This is the second time in around two months when researchers have discovered flaws in Netgear routers. Just last month, the US-CERT advised users to stop using Netgear's R7000 and R6400 routers due to a serious bug that permitted command injection.

However, in an effort to make its product safe, Netgear recently partnered up with Bugcrowd to launch a bug bounty program that can earn researchers cash rewards of up to $15,000 for finding and responsibly reporting flaws in its hardware, APIs, and the mobile apps. -Courtesy of SynEVOL
