Microsoft warns of serious vulnerabilities in Netgear's DGN2200v1 router

theregister.com/2021/07/01/microsoft_netgear_security_advisory_dgn2200v1

Security

Gadget capable of 'opening the gates for attackers to roam untethered through an entire organisation'

Gareth Halfacree Thu 1 Jul 2021 // 17:45 UTC

Netgear has patched serious security vulnerabilities in its DGN2200v1 network router, following the discovery of "very odd behaviour" by a Microsoft security research team - a somewhat understated way of saying that attackers can gain "complete control over the router."

Unveiled by the company at the Consumer Electronics Show back in 2010, Netgear's DGN2200 is an ADSL modem-router combo box with, the company promised at the time, security features including "live parental controls, firewall protection, denial-of-service (DoS) attack prevention, [and] intrusion detection and prevention (IDS)."

Sadly, one thing didn't make the list: functional authentication. As a result, it's possible for remote attackers to take over the router at any time - as discovered by members of the Microsoft 365 Defender Research Team.

"We discovered the vulnerabilities while researching device fingerprinting in the new device discovery capabilities in Microsoft Defender for Endpoint," the research team said. "We noticed a very odd behaviour: a device owned by a non-IT personnel was trying to access a NETGEAR DGN2200v1 router's management port.

"The communication was flagged as anomalous by machine learning models, but the communication itself was TLS-encrypted and private to protect customer privacy, so we decided to focus on the router and investigate whether it exhibited security weaknesses that can be exploited in a possible attack scenario."

The answer, it turns out, is yes - and how. The three core vulnerabilities discovered by Microsoft, rated high-to-critical severity with CVSS scores ranging from 7.1 to 9.4, have been described in no lesser terms than "opening the gates for attackers to roam untethered through an entire organisation."

The core issue behind the vulnerabilities is an authentication bypass flaw, the result of sloppy coding which makes it possible to access any resource on the router simply by including a substring in an HTTP GET request.

Once exploited, further vulnerabilities allow for security credentials - both those for the router and those for its WAN-side network connection - to be retrieved.

This isn't the first time Netgear has been caught with its security pants down, either - nor even the first this year. Back in March the NCC Group warned of 15 serious vulnerabilities in the Netgear JGS516PE Ethernet switch, its devices were implicated as being vulnerable to the DNSpooq attack, and in February SonicWall fingered the DGN1000 and DGN2200 as under active attack from vulnerabilities very similar to those discovered by Microsoft - the patch for which apparently failed to take.

"Third-party routers are often the way to go to own more control, but it doesn't always mean they are bulletproof," Jake Moore, cybersecurity expert at ESET UK, told *The Register*.

"Although it would be worst-case scenario that any connected devices were to be attacked, this highlights that people must stay alert to such threats and to keep on top of patching all devices. And, of course, it is recommended to download and update to the latest firmware for this Netgear router to protect your network."
