Bloomberg alleges Huawei routers and network gear are backdoored

Enlarge / PORTUGAL – 2019/03/04: 5G logo is seen on an android mobile phone with Huawei logo on the background.

reader comments

114 with 71 posters participating

Share this story

Vodafone, the largest mobile network operator in Europe, found backdoors in Huawei equipment between 2009 and 2011, reports Bloomberg. With these backdoors, Huawei could have gained unauthorized access to Vodafone's "fixed-line network in Italy." But Vodafone disagrees, saying that while it did discover some security vulnerabilities in Huawei equipment, these were fixed by Huawei and in any case were not remotely accessible, and hence they could not be used by Huawei.

Bloomberg's claims are based on Vodafone's internal security documentation and "people involved in the situation." Several different "backdoors" are described: unsecured telnet access to home routers, along with "backdoors" in optical service nodes (which connect last-mile distribution networks to optical backbone networks) and "broadband network gateways" (BNG) (which sit between broadband users and the backbone network, providing access control, authentication, and similar services).

In response to Bloomberg, Vodafone said that the router vulnerabilities were found and fixed in 2011 and the BNG flaws

were found and fixed in 2012. While it has documentation about some optical service node vulnerabilities, Vodafone continued, it has no information about when they were fixed. Further, the network operator said that it has no evidence of issues outside Italy.

The sources speaking to Bloomberg contest this. They claim that the vulnerabilities persisted after 2012 and that the same flaws could be found in Vodafone-deployed Huawei equipment in the UK, Germany, Spain, and Portugal. In spite of this, Vodafone continued to buy equipment from the Chinese firm because it was so cost competitive.

The sources also claim that the story was not so simple as "Vodafone reports bug, Huawei fixes bug." Vodafone Italy found that Huawei's routers had unsecured telnet access, and the company told Huawei to remove it. Huawei told Vodafone that it had done so, but further examination of the routers found that telnet could be re-enabled. Vodafone told Huawei that Vodafone wanted it removed entirely, only to be told by Huawei that the company needed to keep it for testing and configuration.

The Bloomberg report doesn't offer any detail on the other alleged "backdoors" in the gateways or service nodes.

When is a front door a backdoor?

The accuracy of Bloomberg's report hinges on the distinction between a vulnerability and a backdoor. A vulnerability is an accidental coding error that permits unauthorized parties to access the router (or other hardware). A backdoor, in contrast, is a deliberately written piece of code that permits unauthorized parties to access the router. While a backdoor could be written such that it's obvious that it's a backdoor (for example, one could imagine an authentication system that allowed anyone to log in with the password "backdoor"), any competent backdoor will look either like a legitimate feature or an accidental coding error.

Telnet access, for example, is a common feature of home routers. Typically, the telnet interface gives greater control over the router's behavior than is available through the Web-based configuration interface that these devices usually have. The telnet interface is also easier to automate, making it easier to preconfigure the devices so that they're properly set up for a particular ISP's network. Even Huawei's initial response to Vodafone's request, which allowed users to re-enable the telnet service, isn't out of the ordinary: it's common for the Web front-ends to allow telnet to be turned off and on. Vodafone's assertion that the telnet service wasn't accessible from the Internet is also likely to be true; typically, these telnet services are only accessible from the local network side, not from the Internet IP address.

As such, Vodafone and Huawei's posture that this isn't a backdoor at all is entirely defensible, and Huawei has done nothing that's particularly out of the ordinary. This is not to say that the hardware is not backdoored—routers with unauthenticated remote access or bypassable authentication have been found in the past and are likely to be found in the future, too. But there's no indication that these particular Huawei issues are an attempt to backdoor the routers, and nothing in the Bloomberg report corroborates this specific claim.

What there is, however, is a concern fueled by the US government that Huawei wishes to compromise or undermine networks and systems belonging to the US and Europe, as well as a concern that the company tries to unlawfully use intellectual property taken from Western countries. Among Chinese firms, Huawei is viewed with particular suspicion due to its ties to the Chinese military.

Huawei's CFO was arrested in Canada on behalf of the United States, which says that Huawei has violated the US sanctions against Iran, and the company has also been indicted for stealing robotic phone-testing technology from T-Mobile. The

US government has pressured domestic companies to not buy or sell Huawei hardware, and more broadly, the US has pushed its allies to avoid Huawei network hardware. Examination of Huawei's firmware and software by the UK government has revealed a generally shoddy approach to security, but these problems appear to be buggy code that was carelessly written and leaves systems hackable rather than deliberate insertion of backdoors.

This pressure is particularly acute when it comes to deploying 5G networks. Huawei's 4G hardware is already widely deployed in Europe, and Huawei's 5G hardware is aggressively priced and seen as critical to the timely deployment of 5G infrastructure in Europe. Vodafone, for its part, continued to buy Huawei gear until January of this year; further purchases have been paused because of the concerns about the company.

https://arstechnica.com/?p=1498049

Local Credit Union Sues Fiserv Over 'Amateurish Security Lapses'

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5e2-JQpYRcc/local-credit-union-sues-fiserv-over-amateurish-security-lapses

---

New Sodinokibi Ransomware Delivered via Oracle WebLogic Flaw

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/1dL5wptogtw/new-sodinokibi-ransomware-delivered-oracle-weblogic-flaw

---

Vodafone Identified Huawei Security Flaw Decade Ago

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/elVXF4EUBWY/vodafone-identified-huawei-security-flaw-decade-ago

---

ImmuniWeb Launches Free Testing Tool for Website Security and PCI Compliance

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/z3CgsfrH93Y/immuniweb-launches-free-testing-tool-website-security-and-pci-compliance

Oracle Patches WebLogic Zero-Day Exploited in Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Ej550C03lwQ/oracle-patches-weblogic-zero-day-exploited-attacks

---

AESDDoS Botnet Targets Vulnerability in Atlassian’s Confluence Server

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/s01qbGyXkAY/aesddos-botnet-targets-vulnerability-atlassian%E2%80%99s-confluence-server

---

P2P Flaws Expose Millions of IoT Devices to Remote Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/gdEK4F0KNl0/p2p-flaws-expose-millions-iot-devices-remote-attacks

Cisco Finds Serious Flaws in Sierra Wireless AirLink Devices

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/FE82oY5_8iM/cisco-finds-serious-flaws-sierra-wireless-airlink-devices

---

NIST Tool Finds Errors in Complex Safety-Critical Software

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/RWGONLRndRg/nist-tool-finds-errors-complex-safety-critical-software