The Daily Swig
Cybersecurity news and views

Decade-long vulnerability in multiple routers could allow network compromise

Jessica Haworth 04 August 2021 at 15:53 UTC
Updated: 05 August 2021 at 11:13 UTC

Vulnerabilities Hardware Authentication

Devices using Arcadyan software are at risk

UPDATED A 12-year-old authentication bypass vulnerability that could allow attackers to compromise networks and devices has been discovered in at least 20 router models, potentially affecting millions of users.

Discovered by Evan Grant of Tenable, the critical path traversal flaw is tracked as CVE-2021–20090, with a CVSS of 9.8, and is exploitable by unauthenticated, remote attackers.

Grant found the issue, which has been present for at least 12 years, in Buffalo routers, specifically the Arcadyan-based web interface software.

Bug hunting

In a blog post, the researcher explained that one of the first things he looks at while analyzing any web application or interface is how it handles authentication.

Grant found that the feature `bypass_check()` was only checking as many bytes as are in `bypass_list` strings.

Grant wrote: “This means that if a user is trying to reach http://router/images/someimage.png, the comparison will match since `/images/` is in the bypass list, and the URL we are trying to reach begins with `/images/`.

“The `bypass_check()` function doesn’t care about strings which come after, such as ‘someimage.png’.

“So what if we try to reach `/images/../<somepagehere>`? For example, let’s try `/images/..%2finfo.html`. The `/info.html` URL normally contains all of the nice LAN/WAN info when we first login to the device, but returns any unauthenticated users to the login screen.”

Read more of the latest security vulnerability news

Grant was able to exploit this vulnerability to bypass authentication, allowing an unauthenticated user to access pages they shouldn’t be able to.

Two other vulnerabilities, CVE-2021-20091 and CVE-2021-20092, were found that currently are only known to affect specific Buffalo routers.

Grant told *The Daily Swig*: “CVE-2021-20091 would allow an authenticated attacker (or one leveraging the aforementioned authentication bypass) to gain root access to the device by injecting a line into the router’s

Latest Posts

HTTP/2 flaws expose organ
to fresh wave of request sm
attacks
Security researcher James Kettle
into the web stack to reveal some
new attack surface

Lessons from the aviation se
after Biden mandates cyber-
investigatory body
‘We might not make cyber-attacks
as airline disasters, but we can ho
make them a more manageable pr

Black Hat Briefings
Hosted DNS config flaws risk leaki
corporate network details

configuration file, which enables the telnet service upon reboot.

“CVE-2021-20092 allows unauthenticated attackers to read sensitive configuration settings including, for certain models, the admin password to the web interface.”

The issue has since been patched in Buffalo WSR-2533DHPL2 devices, prior to and including firmware version 1.02, and WSR-2533DHP3 prior to and including version 1.24.

More vulnerable devices

After confirming the vulnerability was present in the Buffalo router, Grant said that he discovered it also affected at least 20 other models.

“This [vulnerability] appears to be shared by almost every Arcadyan-manufactured router/modem we could find, including devices which were originally sold as far back as 2008,” wrote Grant.

Grant said this latest discovery sparks concern around the risk of supply chain attacks, an ever-increasing and serious threat to organizations and technology users.

“There is a much larger conversation to be had about how this vulnerability in Arcadyan’s firmware has existed for at least 10 years and has therefore found its way through the supply chain into at least 20 models across 17 different vendors,” Grant wrote.

He told *The Daily Swig* that the vulnerabilities were “fairly easy to discover” and “trivial to exploit.

“Consequently, we were surprised they hadn’t been discovered and fixed by the manufacturer or vendors who are selling affected devices over the past decade,” Grant added.

MUST READ Four-fold increase in software supply chain attacks predicted in 2021 – report

“The authentication bypass vulnerability exists due to a list of folders which fall under a ‘bypass list’ for authentication, and improper validation of the paths being provided, leading to the path traversal.

“For most of the devices listed, that means that the vulnerability can be triggered by multiple paths.

“The severity of the flaw depends on other vulnerabilities within the device, such as CVE-2021-20091 present in the Buffalo router that grants root access.

“At least two different vendors were found to have other vulnerabilities unique to their own devices that an attacker could potentially daisy-chain for further exploitation.”

The researcher also noted that this latest disclosure is “an important lesson in how one should approach research on consumer electronics”.

He added: “The vendor selling you the device is not necessarily the one who manufactured it, and if you find bugs in a consumer router’s firmware, they could potentially affect many more vendors and devices than just the one you are researching.”

This article has been updated to include additional comments from Evan Grant, who discovered the vulnerabilities.

RELATED Aaron Portnoy – ‘There’s no silver bullet for ransomware or supply chain attacks’

Vulnerabilities | Hardware | Authentication | Supply Chain Attacks | US | Network Security | North America | Hacking News | Hacking Techniques | Path Traversal | Secure Development

Jessica Haworth

@JesscaHaworth

Related stories

HTTP/2 flaws expose organizations to fresh wave of request smuggling attacks

Security researcher James Kettle digs deep into the web stack to reveal some shiny new attack surface

05 August 2021

Lessons from the aviation sector after Biden mandates cyber-attack investigatory body

05 August 2021

Black Hat Briefings

Hosted DNS config flaws risk leaking corporate network details

05 August 2021

Credential leak detection

Scrapesy aims to reduce incider response times

05 August 2021

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers

Organizations
Testers
Developers

Company

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research
The Daily Swig

PortSwig

Follow us