tenable

IgniteNet HeliOS GLinq v2.2.1 r2961 Multiple Vulnerabilities

Medium

← View More Research Advisories

Synopsis

CVE-2020-5781 - Cross-site scripting and Denial of Service

CVSSv2 Base Score: 5.5
CVSSv2 Vector: (AV:N/AC:L/Au:S/C:N/I :P/A:P)

It was noted during testing that when a user logs in the langSelection parameter is stored in the luci configuration file (/etc/config/luci) by the authenticator.htmlauth function from /usr/lib/lua/luci/dispatcher.lua.

A user is able to inject javascript into this parameter which makes the web interface completely unusable by anyone who is currently logged in. Aside from triggering the injected javascript whenever a user makes an action on the device's web user interface, it also prevents anyone from logging in until this issue is manually resolved by modifying the /etc/config/luci file.

Proof of concept

When browsing to the below URL (assuming the credentials and IP address are correct) we inject javascript in every page in the web user interface by adding our payload to the 'langSelection' parameter.

http://<host>/cgi-bin/acn?username=root&login_msg=&password=admin123&langSelection="<script>alert('1337+hacks')</script>

==========

CVE-2020-5782 - Denial of Service

CVSSv2 Base Score: 6.8
CVSSv2 Vector: (AV:N/AC:L/Au:S/C:N/I:N/A:C)

During testing it was noted that there is a parameter accepted during the login process called 'wan_type':

If a user logs in and sets the 'wan_type' parameter to anything, then whatever is added will be written to the 'proto' for the wan interface network configuration and applied. This will essentially break the wan interface leaving the device unreachable over ethernet until someone is able to manually edit the /etc/config/network configuration file.

Proof of concept

To test this issue browse to the below URL (assuming the IP address and credentials are correct):

http://<host>/cgi-bin/acn?username=root&login_msg=&password=admin123&langSelection=en&wan_type=anything

The device will then become unreachable.

==========

CVE-2020-5783 - Cross-site request forgery

CVSSv2 Base Score: 5.5
CVSSv2 Vector: (AV:N/AC:L/Au:S/C:P /I:P /A:N)

There is no CSRF protection on the login form for this device, An unauthenticated attacker could spoof the login page and trick a legitimate user to login to their page instead of the real one. This is usually not considered a serious issue but combined with the Stored XSS/Dos findings within the authentication process this should be fixed.

Proof of concept

The below html can be used as a proof of concept.

```
<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://CHANGEMEcgi-bin/acn">
<input type="hidden" name="username" value="root" />
<input type="hidden" name="login_msg" value="" />
<input type="hidden" name="password" value="admin123" />
<input type="hidden" name="langSelection" value=""<script>alert('1337 hacks')</script>" />
<input type="submit" value="Login" />
</form>
</body>
</html>
```

When selecting 'Login' a request will be made to the specified device web user interface. This would not be possible if CSRF protection was in place.

If the language parameter is changed from the default 'en' to 'anything' an error will be triggered.

When inspecting the HTML of the page at this point the 'anything' string is present in the page.

This could potentially lead to XSS or other injection vulnerabilities.

Solution

No solution has been provided by the vendor.

Disclosure Timeline

June 23, 2020 - Tenable requests security contact from vendor.
June 30, 2020 - Tenable requests security contact from vendor (attempt 2).
July 7, 2020 - Tenable requests security contact from vendor (attempt 3).
August 18, 2020 - Tenable reports to CERT.

Risk Information

CVE ID: CVE-2020-5781
CVE-2020-5782
CVE-2020-5783
Tenable Advisory ID: TRA-2020-55
Credit: Derrie Sutton

CVSSv2 Base / Temporal Score: 6.8 / 5.5
CVSSv2 Vector: AV:N/AC:L/Au:S/C:N/I:N/A:C
Affected Products: IgniteNet HeliOS GLinq v2.2.1 r2961
Risk Factor: Medium

Advisory Timeline

September 22, 2020 - Initial release.

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

tenable