Teltonika Gateway TRB245 Stored Cross-site Scripting

Low

← View More Research Advisories

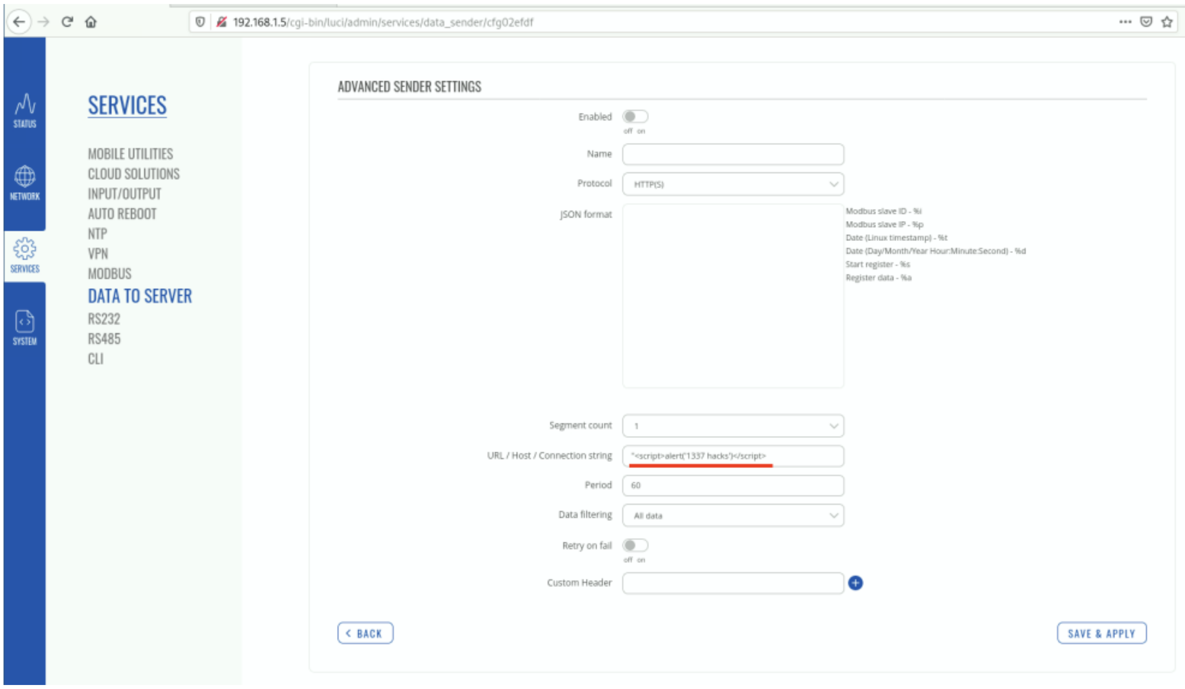
Synopsis

A stored cross-site scripting vulnerability exists in the Web UI. A remote, authenticated attacker is able to inject malicious client-side code into the 'URL/ Host / Connection' form in the 'DATA TO SERVER' configuration section. An attacker with low privileges could exploit this to steal session details from a higher privileged user.

Proof of Concept

In the below screenshot we can see the tester has added some script tags into the 'URL/ Host / Connection' form.

```
"<script>alert('1337 hacks')</script>
```



192.168.1.5/cgi-bin/luci/admin/services/data_sender/cfg02efdf

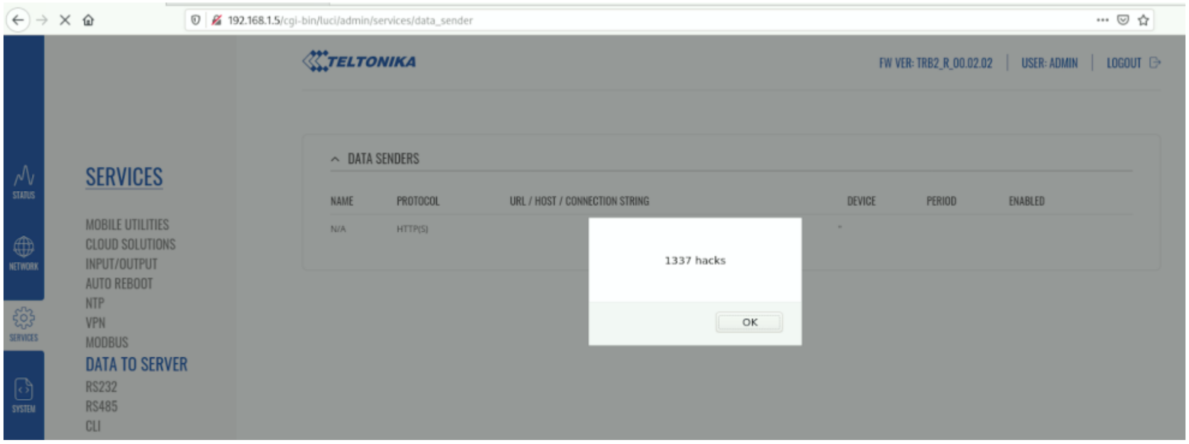
ADVANCED SENDER SETTINGS

Enabled: off on
Name:
Protocol: HTTP(S)
JSON format:

Modbus slave ID - %i
Modbus slave IP - %p
Date (Linux timestamp) - %t
Date (Day/Month/Year Hour:Minute:Second) - %d
Start register - %s
Register data - %a

Segment count: 1
URL / Host / Connection string: "<script>alert('1337 hacks')</script>
Period: 60
Data filtering: All data
Retry on fail: off on
Custom Header:

When the tester selects 'Save & Apply' this change you will be redirected to the list of data sensors and the injected javascript will execute.



192.168.1.5/cgi-bin/luci/admin/services/data_sender

DATA SENDERS

NAME	PROTOCOL	URL / HOST / CONNECTION STRING	DEVICE	PERIOD	ENABLED
N/A	HTTP(S)		"		

1337 hacks

Solution

Upgrade to TRB2_R_00.02.03 or newer.

Additional References

https://wiki.teltonika-networks.com/view/TRB245_Firmware_Downloads#TRB2XX_R_00.02.03.1_.7C_2020.05.15

Disclosure Timeline

07/09/2020 - Teltonika thanks us for the report. They will investigate and follow up with us. They do ask us for a PoC as well.
07/09/2020 - Teltonika responds with their initial assessment.
07/09/2020 - Tenable thanks Teltonika for the update. Sends PoC over.
07/10/2020 - Teltonika cannot reproduce XSS on the newest firmware TRB2_R_00.02.04.
07/10/2020 - Tenable asks if XSS was confirmed to exist in TRB2_R_00.02.02 firmware.
07/14/2020 - Teltonika can reproduce the vulnerability in TRB2_R_00.02.02 firmware.
07/14/2020 - Since the vulnerability was confirmed in a previous version, Tenable will plan to assign a CVE and release an advisory. Asks if a CVE has already been assigned and which version corrected the issue.
07/16/2020 - Teltonika says they did not assign a CVE. Fix version is TRB2_R_00.02.03.
07/16/2020 - We will publish the XSS as CVE-2020-5769 and send a link to the advisory after it is published.

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-2020-5769
Tenable Advisory ID: TRA-2020-43
Credit: Derrie Sutton

CVSSv2 Base / Temporal Score: 3.6
CVSSv2 Vector: AV:N/AC:H/Au:S/C:P/I:P/A:N
Affected Products: TRB2_R_00.02.02 firmware
Risk Factor: Low

Advisory Timeline

07/16/2020 - Advisory published.
07/29/2020 - Revised disclosure timeline per discussion with Teltonika.

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

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust