dSA-201101: Multiple Vulnerabilities in dLAN Green PHY Module SDK IP stack

Published: 2020-12-08
Document version: 1.1

Notice

devolo AG is aware of multiple security vulnerabilities in the "uIP" stack which is used in older versions of the devolo dLAN Green PHY Module SDK and bootloader. Exploitation of these vulnerabilities could cause denial of service, DNS cache poisoning or remote code execution.

The dLAN Green PHY Modules are shipped with a LPC1758 firmware (v1.0.16) which is only doing bridging between Ethernet and PLC. This firmware does not include an IP stack and is therefore **not** affected.

The firmware of the Green PHY chip (QCA7000) is also **not** affected.

The information in this document is subject to change without notice and should not be construed as a commitment by devolo AG. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

Affected Product and Version

devolo dLAN Green PHY Module SDK
Version 1.0.16 and earlier

devolo dLAN Green PHY Module bootloader
Version 1.0.16 and earlier

Vulnerability Details

CVE-2020-13988

CWE ID: CWE-190

Description: The routine for parsing TCP MSS options relies on a `uint8_t` counter that under certain conditions will be only mutated depending on an arbitrary MSS option's length value. If that length value is `0xff`, the counter will be decremented and thus pointing on a value according to which the counter will be incremented. This will go one infinitely resulting in an infinite loop.

CVE-2020-13987

CWE ID: CWE-125

Description: When calculating the checksum for IP data, the function in question doesn't check the validity of the `length field` of the `upper layer (TCP/UDP)` segment against the length of the internal buffer `uip_buf`. That would result eventually into an `Out of bounds read` bug which might result in a crash `DoS`. The crash depends on how the platform implements memory protection and the `out of bound read`'s size.

CVE-2020-17438

CWE ID: CWE-787

Description: The code that reassembles fragmented packets fails to properly validate the total length of an incoming packet specified in its IP header, as well as the fragmentation offset value specified in the IP header. By crafting a packet with specific values of the IP header length and the fragmentation offset, attackers can write into the `.bss` section of the program past the statically allocated buffer that is used for storing the fragmented data, and cause a DoS/RCE (RCE highly depends on the architecture of the target platform).

CVE-2020-17440

CWE ID: CWE-476

Description: The code that parses incoming DNS packets does not validate that domain names present in the DNS responses are NULL terminated. This results in errors when calculating the offset of the pointer that jumps over domain name bytes in DNS response packets when domain names are not NULL terminated, and eventually leads to dereferencing the pointer at an invalid address.

CVE-2020-17439

CWE ID: CWE-923

Description: The code that parses incoming DNS packets does not validate that the incoming DNS replies match outgoing DNS queries, and arbitrary DNS replies are parsed if there was ANY outgoing DNS query with transaction id that matches the transaction id of an incoming reply. Provided that the default DNS cache is quite small (only four records) and that the transaction id has a very limited set of values that is quite easy to guess, this can lead to DNS cache poisoning.

CVE-2020-17437

CWE ID: CWE-125

Description: When TCP Urgent flag is set in a TCP packet, and the stack is configured to ignore the urgent data, the stack will attempt to use the value of the Urgent pointer bytes to separate the Urgent data from the normal data by calculating the offset at which the normal data should be present in the global buffer. The problem is that the length of this offset is not checked, therefore for large values of the Urgent pointer bytes, the data pointer can point to some memory that is way beyond the data buffer. Also, the length of the normal TCP data is not validated.

CVE-2020-24334

CWE-ID: CWE-125

Description: The code that processes DNS responses in uIP, Contiki-OS, and Contiki-NG does not check whether the number of responses specified in the DNS packet header correspond to the response data available in the DNS packet, leading to Out-of-bounds read, and Denial-of-Service consequently.

CVE-2020-24335

CWE-ID: CWE-125

Description: The decompression of a domain name doesn't check if the name pointer points within the bound of the actual packet, which can result in an out of bounds read and eventually triggering the memory protection unit resulting in a DoS.

Impact

The dLAN Green PHY Module bootloader only does UDP and ARP, not TCP or DNS, and fragmentation is not supported. The bootloader is only active when the module restarts, and only for three seconds, on the Ethernet interface, requesting a TFTP download from a not publicly routable, private class C IP address. For the TFTP Get request the bootloader uses the fixed local IP address 192.168.0.201 and expects the TFTP server at the fixed IP address 192.168.0.5. For these reasons, the risk of it being susceptible to the remaining CVE-2020-13987 is therefore deemed very low.

The dLAN Green PHY Module firmware that comes pre-installed on the modules is not affected by the above vulnerabilities, as it does not include an IP stack.

Customers who have developed a custom firmware based on the devolo dLAN Green PHY SDK may be susceptible to any or all of the above vulnerabilities, depending on their use of the SDK's IP stack.

Remediation and Mitigation

For customers who have developed custom firmware based on the dLAN Green PHY SDK, devolo AG recommends, to update to the current dLAN Green PHY SDK, version 3.2.0 or higher. This version does not use the "uIP" stack anymore and is thus not affected by the vulnerabilities above.

It is available from https://github.com/devolo/dlan-greenphy-sdk/releases

devolo AG does not plan to release an update of the bootloader, due to the very low risk of exploitation. Customers are generally advised to take appropriate measures to protect access to the LAN that the device is operated in. TFTP communication should be restricted to legitimate network partners, e.g. by using a firewall and robust network segmentation.

Acknowlegements

devolo AG thanks the following parties for their efforts:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) for coordinated disclosure
- Cybersecurity and Infrastructure Security Agency (CISA) for coordinated disclosure
- Joe Wetzels, Stanislav Dashevskyi, Amine Amri and Daniel dos Santos at Forescout Technologies for identifying and reporting these vulnerabilities

Revision History

Version 1.1 (2020-12-08) – added note, that QCA7000 firmware is not affected

Version 1.0 (2020-12-07) – initial version