Out-of-bounds write when processing 6LoWPAN extension headers

Moderate joakimeriksson published GHSA-r768-hrhf-v592 on Jun 18, 2021

Package

Contiki-NG

Affected versions	Patched versions
< 4.6	4.6

Description

Impact

It is possible to cause an out-of-bounds write in Contiki-NG when transmitting a 6LoWPAN packet with a chain of extension headers. Unfortunately, the written header is not checked to be within the available space, thereby making it possible to write outside the buffer.

The statement causing the buffer overlow is on line 1274 in the os/net/ipv6/sicslowpan.c module:

```
memcpy((uint8_t*)exthdr + 2, hc06_ptr, len);
```

In this statement, the exthdr variable points into the uncompressed packet buffer, where an extension header pointed to by the `hc06_ptr` variable is written. The buffer overflow can occur because the lack of validation of the len variable, which is read from the compressed input packet.

Patches

The problem has been patched in Contiki-NG 4.6.

Workarounds

Users can apply the patch in Contiki-NG PR #1409.

For more information

If you have any questions or comments about this advisory:

- Open an issue in https://github.com/contiki-ng/contiki-ng/
- Email us at security@contiki-ng.org

Severity

Moderate

CVE ID

CVE-2021-21280

Weaknesses

No CWEs