

New issue

Jump to bottom

Out of bounds memory access in SNMP BER decoder/encoder routines #1354

Open mjurczak opened this issue on Aug 17, 2020 · 1 comment

Labels bug/vulnerability

mjurczak commented on Aug 17, 2020

Contributor

Description of defect

References:

<https://github.com/contiki-ng/contiki-ng/tree/release/v4.5>
<https://github.com/contiki-ng/contiki-ng/tree/release/v4.4>

File:

[snmp-engine.c](#)

Analysis:

Memory access out of buffer boundaries may occur if an SNMP ASN.1 BER encoder/decoder routines.

The length of provided input/output buffers is insufficiently verified when encoding and decoding data. Lack of boundary checks may lead to out-of-bounds buffer read or write access.

Example functions that make access to memory without prior verification of sufficient input data length:

[contiki-ng/os/net/app-layer/snmp/snmp-ber.c](#)
Line 129 in 31753fe

```
129 snmp_ber_decode_type(unsigned char *buff, uint32_t *buff_len, uint8_t *type)
```

[contiki-ng/os/net/app-layer/snmp/snmp-ber.c](#)
Line 138 in 31753fe

```
138 snmp_ber_decode_length(unsigned char *buff, uint32_t *buff_len, uint8_t *length)
```

[contiki-ng/os/net/app-layer/snmp/snmp-ber.c](#)
Line 147 in 31753fe

```
147 snmp_ber_decode_integer(unsigned char *buf, uint32_t *buff_len, uint32_t *num)
```

[contiki-ng/os/net/app-layer/snmp/snmp-ber.c](#)
Line 183 in 31753fe

```
183 snmp_ber_decode_unsigned_integer(unsigned char *buf, uint32_t *buff_len, uint8_t expected_type, uint32_t *num)
```

[contiki-ng/os/net/app-layer/snmp/snmp-ber.c](#)
Line 264 in 31753fe

```
264 snmp_ber_decode_null(unsigned char *buf, uint32_t *buff_len)
```

Type:

- Out-of-bounds memory access

Result:

- Memory corruption
- Invalid memory read access

Target(s) affected by this defect ?

- contiki-ng v4.5
- contiki-ng v4.4

mjurczak mentioned this issue on Aug 17, 2020

Bugfix/snmp engine #1355

Merged

Yagoor mentioned this issue on Sep 8, 2020


SNMP Engine - New Unit Tests #1376

Closed

g-oikonomou commented on Nov 25, 2020

Member

@Yagoor @mjurczak: Am I right to assume that this has been fixed in #1355 and/or #1397? Can we close?

  **g-oikonomou** added the `bug/vulnerability` label on Nov 25, 2020

Assignees

No one assigned

Labels

`bug/vulnerability`

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

