Jump to bottom

Buffer overflow in .bss section due to SNMP request overflow #1352

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
snmp-message.c

Analysis:
Memory access out of buffer boundaries may occur if an SNMP request with number of OIDs larger than supported by the engine is received and processed.

The OIDs listed in a request are processed by snmp_message_decode() function without verification of the varbinds buffer capacity.
The buffer is allocated in .bss as a static variable:

contiki-ng/os/net/app-layer/snmp/snmp-engine.c
Line 208 in 23db957

```
208      static snmp_varbind_t varbinds[SNMP_MAX_NR_VALUES];
```

The varbinds memory buffer is written with the values provided in SNMP request:

contiki-ng/os/net/app-layer/snmp/snmp-message.c
Line 245 in 23db957

```
245      buf = snmp_oid_decode_oid(buf, &buf_len, varbinds[i].oid, &oid_len);
```

The buffer capacity is determined at compile time by the following definition:

contiki-ng/os/net/app-layer/snmp/snmp-conf.h
Lines 81 to 87 in 23db957

```
81      #define SNMP_MAX_NR_VALUES SNMP_CONF_MAX_NR_VALUES
82      #else
83      /**
84       * \brief Default maximum number of OIDs in one response
85       */
86      #define SNMP_MAX_NR_VALUES 2
87      #endif
```

If the number of variables in the request exceeds the allocated buffer a memory write out of the buffer boundaries occurs. The write operation beyond the buffer capacity provides possibility to overwrite other variables allocated in the .bss section by the application.
As the sender of the frame is in controll of the content that will be written beyond the buffer limits and there is no strict process memory separation in contiki-ng, this issue may allow overwriting of sensitive memory areas of IoT device.

Type:

- Out-of-bounds memory write

Result:

- Memory corruption
- Memory write to initialized variables segment with arbitrary data

Target(s) affected by this defect ?

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

Fix

Rudimentary fix to address the most critical aspect of the issue:
https://github.com/mjurczak/contiki-ng/tree/bugfix/snmp-engine

How is this defect reproduced ?

An example hex-encoded SNMP request causing out-of-bounds memory write to varbinds:

```
3060020100040670756 26C6963A0530201290201000201003048301606122B06010401817D0840040201070A86DEB7380500301606122B06010401817D084004
0201070A86DEB7360500301606122B06010401817D0840040201050A86DEB9600500
```

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