~~Bug 1202023 - (CVE-2022-37032) VUL-0: CVE-2022-37032: frr: out-of-bounds read in the BGP daemon may lead to information disclosure or denial of service~~

Status: RESOLVED FIXED

Classification: Novell Products
Product: SUSE Security Incidents
Component: Incidents
Version: unspecified
Hardware: Other Other

Priority: P3 - Medium **Severity**: Normal
Target Milestone: ---
Assigned To: Security Team bot
QA Contact: Security Team bot

URL: https://smash.suse.de/issue/338551/
Whiteboard: CVSSv3.1:SUSE:CVE-2022-37032:7.1:(AV:...
Keywords:

Depends on: ~~1196957~~
Blocks:

Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2022-08-01 10:25 UTC by Carlos López
Modified: 2022-10-13 14:50 UTC (History)
CC List: 4 users (show)

See Also:
Found By: Security Response Team
Services Priority:
Business Priority:
Blocker: ---

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

Carlos López 2022-08-01 10:25:45 UTC Description

```
When FRR receives a BGP capability message, the following call trace occurs when an
attempt is made to parse it:

```
#0 bgp_capability_msg_parse() in bgpd/bgp_packet.c
#1 bgp_capability_receive() in bgpd/bgp_packet.c
#2 bgp_process_packet() in bgpd/bgp_packet.c
```

In `bgp_capability_msg_parse()`, an inproper calculation on the bounds of the
available data is made.
```

```c
static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,
                                    bgp_size_t length)
{
        ...
        end = pnt + length;

        while (pnt < end) {
                /* We need at least action, capability code and capability
                 * length. */
                if (pnt + 3 > end) {
                        /* error ... */
                }
                ...
                hdr = (struct capability_header *)(pnt + 1);

                ...

                /* Capability length check. */
                if ((pnt + hdr->length + 3) > end) {
                        /* error ... */
                }

                /* Fetch structure to the byte stream. */
                memcpy(&mpc, pnt + 3, sizeof(struct capability_mp_data));
                pnt += hdr->length + 3;

        }

        return BGP_PACKET_NOOP;
}
```

While the first length check is properly done, the second one relies on a value directly read from the packet without verification. `hdr->length` is used to check the remaining amount of data, but the actual amount read is `sizeof(struct capability_mp_data)`. This means that the size check can be bypassed, causing `memcpy()` to read out of bounds.

This issue could be exploited to trigger a segmentation fault, leading to denial of service, or cause undefined behavior via corrupt fields in `mpc`.

This issue was fixed with the following commit:
https://github.com/FRRouting/frr/commit/ff6db1027f8f36df657ff2e5ea167773752537ed

Carlos López 2022-08-01 12:46:07 UTC Comment 1

```
Affected:
 - SUSE:SLE-15-SP3:Update
 - openSUSE:Factory
```

Marius Tomaschewski 2022-09-06 10:26:16 UTC Comment 4

Submission request to SLE in https://build.suse.de/request/show/279073

Marius Tomaschewski 2022-09-06 10:30:47 UTC Comment 5

Submission request to network is in https://build.opensuse.org/request/show/1001418

Marius Tomaschewski 2022-09-06 14:49:25 UTC Comment 6

(In reply to Marius Tomaschewski from comment #5)

> Submission request to network is in
> https://build.opensuse.org/request/show/1001418

On the way to factory in https://build.opensuse.org/request/show/1001456

Assigning back to security-team.

Swamp Workflow Management 2022-09-12 10:24:35 UTC Comment 7

SUSE-SU-2022:3246-1: An update that fixes two vulnerabilities is now available.

Category: security (important)
Bug References: 1202022,1202023
CVE References: CVE-2019-25074,CVE-2022-37032
JIRA References:
Sources used:
openSUSE Leap 15.4 (src): frr-7.4-150300.4.7.1
openSUSE Leap 15.3 (src): frr-7.4-150300.4.7.1
SUSE Linux Enterprise Module for Server Applications 15-SP4 (src): frr-7.4-150300.4.7.1
SUSE Linux Enterprise Module for Server Applications 15-SP3 (src): frr-7.4-150300.4.7.1

NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

Carlos López 2022-10-13 14:50:56 UTC Comment 8

Done, closing.