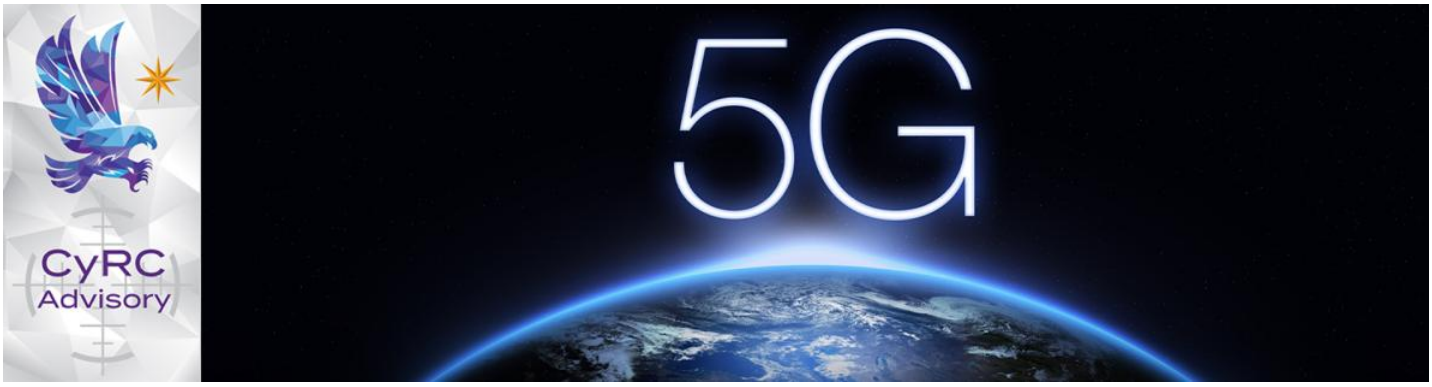
CyRC Vulnerability Advisory: Denial-of-service vulnerabilities (CVE-2022-39063) in Open5GS

Qiang Li

Posted by (https://www.synopsys.com/blogs/software-security/author/qiangl/) on Wednesday, September 14, 2022

CVE-2022-39063 is a vulnerability in the Open5GS project, an open source implementation of 5G components.



The Synopsys Cybersecurity Research Center (CyRC) has exposed a denial-of-service vulnerability in Open5GS. Open5GS is an open source project that provides LTE and 5G mobile packet core network functionalities with an AGPLv3 or commercial license. It can be used to build private LTE/5G telecom networks by individuals or telecom network operators.

When Open5GS UPF receives a `PFCP Session Establishment Request`, it stores related values for building the `PFCP Session Establishment Response`. The following source code in `open5gs/lib/pfcp/handler.c` causes this issue.

```
/* Code block for parsing incoming PFCP Session Establishment Request. */
if (message->pdi.local_f_teid.presence) {
    pdr->f_teid_len = message->pdi.local_f_teid.len;
    memcpy(&pdr->f_teid, message->pdi.local_f_teid.data, pdr->f_teid_len);
    pdr->f_teid.teid = be32toh(pdr->f_teid.teid);
}

...

/* Code block for building outgoing PFCP Session Establishment Response. */
if (pdr->f_teid_len) {
    memcpy(&pdrbuf[i].f_teid, &pdr->f_teid, pdr->f_teid_len);
    pdrbuf[i].f_teid.teid = htobe32(pdr->f_teid.teid);

    message->local_f_teid.presence = 1;
    message->local_f_teid.data = &pdrbuf[i].f_teid;
    message->local_f_teid.len = pdr->f_teid_len;
}
```

Once UPF receives a request, it gets the `f_teid_len` from incoming message, and then uses it to copy data from incoming message to struct `f_teid` without checking the maximum length. If the `pdi.local_f_teid.len` exceeds the maximum length of the struct of `f_teid`, the `memcpy()` overwrites the fields (e.g., `f_teid_len`) after `f_teid` in the `pdr` struct. After parsing the request, the UPF starts to build a response. The `f_teid_len` with its overwritten value is used as a length for `memcpy()`. A segmentation fault occurs if this overwritten value is large enough.

This vulnerability is caused by a `memcpy()` that doesn't have the maximum length of the source and target structure validated, so a buffer overflow attack exploit is possible.

Exploitation

When connecting to the Open5GS UPF port (8805) for the PFCP protocol and sending an `PFCP Association Setup Request` followed by a `PFCP Session Establishment Request` with PDR.F-TEID.IPv6-Address set to a duplicated IPv6 address [e.g., 16(0xff) 16(0xff)], this buffer overflow attack causes a segmentation fault in Open5GS (https://open5gs.org/).

Affected software

Open5GS 2.4.9 and earlier versions

Impact

Exploitation of this vulnerability would lead to a denial-of-service for the LTE/5G mobile packet core network.

CVSS 3.1 base score: 8.2 (high)

CVSS 3.1 vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C (https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C)

Remediation

Synopsys recommends upgrading to Open5GS commit 444e182 or later. The vulnerability is patched as of commit d99491a on August 12, 2022, and commit 444e182 on August 14, 2022.

Discovery credit

Qiang Li from the Synopsys Cybersecurity Research Center (https://www.synopsys.com/software-integrity/cybersecurity-research-center.html) (CyRC) in Wuhan, China, discovered the issue using the Defensics® fuzz testing tool (https://www.synopsys.com/software-integrity/security-testing/fuzz-testing.html).

Timeline

- August 10, 2022: Initial disclosure
- August 16, 2022: Open5GS confirms vulnerability

- August 17, 2022: Synopsys validates the fix
- September 9, 2022: Open5GS version 2.4.10 is released – fixing the bug
- September 14, 2022: Synopsys publishes advisory

About CVSS

FIRST.Org, Inc (FIRST) is a non-profit organization based out of US that owns and manages CVSS. It is not required to be a member of FIRST to utilize or implement CVSS but FIRST does require any individual or organization give appropriate attribution while using CVSS. FIRST also states that any individual or organization that publishes scores follow the guideline so that anyone can understand how the score was calculated.

This post is filed under Security news and research (https://www.synopsys.com/blogs/software-security/category/security-research/).

Qiang Li

Posted by
Qiang Li

Qiang Li is a security-minded senior software engineer at Synopsys. He is of curious nature who likes to per…

SEE AUTHOR ARCHIVE (https://www.synopsys.com/blogs/software-security/author/qiangl)

More from Security news and research

Beyond NVD data: Using Black Duck Security Advisories for version accuracy (https://www.synopsys.com/blogs/software-security/comparing-bdsa-with-nvd-version-accuracy/)

Posted by Lauren Fearon (https://www.synopsys.com/blogs/software-security/author/fearon/) on November 22, 2022

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

The “Software Vulnerability Snapshot” reports that 95% of tests uncovered vulnerabilities in target apps (https://www.synopsys.com/blogs/software-security/software-vulnerability-snapshot-report-findings/)

Fred Bals
Posted by (https://www.synopsys.com/blogs/software-security/author/fbals/) on November 15, 2022

Dynamic application security testing (https://www.synopsys.com/blogs/software-security/tag/dast/)

Penetration testing (https://www.synopsys.com/blogs/software-security/tag/penetration-testing/)

Web application security (https://www.synopsys.com/blogs/software-security/tag/web-application-security/)

CyRC Vulnerability Advisory: CVE-2022-43945 buffer overflow vulnerabilities in NFSD (https://www.synopsys.com/blogs/software-security/cyrc-advisory-buffer-overflow-vulnerabilities-linux-kernel-nfsd/)

Kari Hulkko
Posted by (https://www.synopsys.com/blogs/software-security/author/khulkko/) on November 3, 2022

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

Fuzz testing (https://www.synopsys.com/blogs/software-security/tag/fuzz-testing/)

Experts warn of critical security vulnerability discovered in OpenSSL (https://www.synopsys.com/blogs/software-security/preparing-for-openssl-critical-security-vulnerability/)

Posted by Tim Mackey (https://www.synopsys.com/blogs/software-security/author/tmackey/) on October 28, 2022

Software composition analysis (https://www.synopsys.com/blogs/software-security/tag/software-composition-analysis/)

RELATED TAGS

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

Fuzz testing (https://www.synopsys.com/blogs/software-security/tag/fuzz-testing/)

SEE ALL TAGS

Inclusion & Diversity (/careers/inclusion-diversity.html#present)

Investor Relations (/company/investor-relations.html)

Contact Us (/company/contact-synopsys.html)

FOLLOW

(https://www.linkedin.com/company/synopsys) (https://www.facebook.com/Synopsys) (https://twitter.com/Synopsys)