computer
emergency
response
team
CERT-EU
for the EU institutions, bodies
and agencies

CERT-EU Security Advisory 2017-020

Critical Vulnerabilities Impacting Dnsmasq

October 4, 2017 — v1.0

History:

- *04/10/2017 — v1.0 – Initial publication*

Summary

On October 2nd, 2017, Google published a blog post detailing several critical vulnerabilities impacting **dnsmasq**. Dnsmasq is widely used in Linux and BSD distributions, Android devices and proprietary firmwares for for serving DNS, DHCP, router advertisements, and network boot. It is often exposed to Internet and widely used on internal networks.

Google worked with dnsmasq developers to patch vulnerabilities before releasing proof of concept code [4] and a patch file [5].

The vulnerabilities allow an attacker to perform remote code execution (3 vulnerabilities), to get access to sensitive information (1 vulnerability), or to perform a denial-of-service attack on the service (3 vulnerabilities).

Technical Details

- CVE-2017-14491: DNS-based remote code execution via heap based overflow (2 bytes)
- CVE-2017-14492: DHCP-based remote code execution via heap based overflow – could be used to bypass ASLR if used in combination with CVE-2017-14494
- CVE-2017-14493: DHCP-based remote code execution via stack based overflow
- CVE-2017-14494: DHCP-based Information leak – could be used to bypass ASLR
- CVE-2017-14495: DNS-based denial-of-service
- CVE-2017-14496: DNS-based denial-of-service, also affecting Android
- CVE-2017-13704: DNS-based denial-of-service

Products Affected

- Dnsmasq < 2.78

Recommendations

Fix is available through an upgrade to Dnsmasq version 2.78. [2]

For Android devices, Google released a patch in the October 2017 Security Bulletin [3]. For other Linux and BSD distributions contact your distribution maintainers for a fix.

References

[1] Google blog post https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html

[2] Dnsmasq changelog http://www.thekelleys.org.uk/dnsmasq/CHANGELOG

[3] Android Security Bulletin – October 2017 https://source.android.com/security/bulletin/2017-10-01

[4] Proof of Concept code for vulnerabilities https://github.com/google/security-research-pocs/tree/master/vulnerabilities/dnsmasq

[5] Patch for dnsmasq source code https://github.com/google/security-research-pocs/blob/master/vulnerabilities/dnsmasq/sandbox/dnsmasq-sandbox.patch