Zyxel security advisory for dnsmasq vulnerabilities for North America Region

2017/10/10

The issue

Google has recently reported multiple security vulnerabilities affecting **"Dnsmasq" version 2.77 and earlier versions.** "Dnsmasq" is an open source DNS/DHCP service package commonly used on computers, servers, smartphones, routers, and various networking devices. This is considered as industry-wide security event. This issue is identified in US-CERT vulnerability note VU#973527 with vulnerability IDs below:

- CVE-2017-14491 Heap-based Buffer Overflow
- CVE-2017-14492 Heap-based Buffer Overflow
- CVE-2017-14493 Stack-based Buffer Overflow
- CVE-2017-14494 Information Exposure
- CVE-2017-14495 Uncontrolled Resource Consumption
- CVE-2017-14496 Integer Underflow
- CVE-2017-13704 Integer Underflow

The potential risk

These vulnerabilities can be triggered remotely via DNS and DHCP protocols and can lead to remote code execution, information exposure, and denial of service.

Immune models

DSL CPE	P660HN-51B, P873 series, VSG1432/1435, VMG4325/4380/4381

Affected models and Solution

The table below contains the affected models and patch firmware release schedule. Zyxel encourage our customers to update the field units to this patch firmware to mitigate the risk.

Product	Series/Model	Patch firmware Date
DSL CPE	VMG4825	Oct 23, 2017
	VMG9823	Oct 23, 2017
	VMG3925	Oct 30, 2017
	XMG3512	Nov 15, 2017
	VMG8324	Oct 23, 2017

Zyxel Communications Inc.
1130 N. Miller St, CA 92. Anaheim 806
w: www.zyxel.com/us | e: sales@zyxel.com | t: 800.255.4101 | f: 714.632.0858

Ethernet CPE	EMG2306	Oct 30, 2017
	EMG2926	Oct 23, 2017
	EMG3425	Oct 30, 2017

Where to download patch firmware:

ftp://telcocpesupport.zyxel.com
Username: T3_user
Password: UserDownload900

Please contact your sales representatives or Zyxel support engineering team (bse@zyxel.com) if you require further information or assistance.

[References]

1. Google disclosure
   https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html
2. US-CERT vulnerability note
   http://www.kb.cert.org/vuls/id/973527
3. Red Hat advisory
   https://access.redhat.com/security/vulnerabilities/3199382

Zyxel Communications Inc.
1130 N. Miller St, CA 92. Anaheim 806
w: www.zyxel.com/us | e: sales@zyxel.com | t: 800.255.4101 | f: 714.632.0858