Zyxel is aware of the recently disclosed vulnerabilities of dnsmasq, as identified in US-CERT vulnerability note VU#973527 with vulnerability IDs CVE-2017-14491 through CVE-2017-14496 and CVE-2017-13704, as listed in table 1.

What are the vulnerabilities?

Dnsmasq is a piece of open-source software widely used in Android, Linux and a variety of networking equipment operating systems. The vulnerabilities are present in dnsmasq version 2.77 and earlier; version 2.78 of dnsmasq has been released to address these vulnerabilities.

Table 1

CVE	Issue	Vector
CVE-2017-14491	Heap-based Buffer Overflow	DNS
CVE-2017-14492	Heap-based Buffer Overflow	DHCP
CVE-2017-14493	Stack-based Buffer Overflow	DHCP
CVE-2017-14494	Information Exposure	DHCP
CVE-2017-14495	Uncontrolled Resource Consumption (resource exhaustion)	DNS
CVE-2017-14496	Integer Underflow	DNS

CVE	Issue	Vector
CVE-2017-13704	Integer Underflow	DNS

Please see: https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html for more technical information.

How are Zyxel resolving the vulnerabilities?

At Zyxel we treat security as a top priority and we have conducted a thorough investigation and identified a list of vulnerable products within their warranty and support period, as shown in table 2 below. For products not listed, they are not affected because they do not make use of dnsmasq.

We are now deploying or backporting the latest version of dnsmasq (version 2.78) into the vulnerable products.

Please refer to table 2 for the detailed release schedule. The patch firmware will be available for download at Zyxel Support Center .

Table 2

Product	Series/Model	Patch firmware version	Availability
DSL CPE	AMG1302-T11C	ABCG12C0	Feb 2018
	VMG1312-B10A	AAJZ14C0	Jan 2018

Product	Series/Model	Patch firmware version	Availability
	VMG1312-B10D	V5.13(AAXA.7)	Dec 2017
	VMG1312-B30A	AATO9C0	Jan 2018
	VMG3312-T series	ABFX1C0	Dec 2017
	VMG3625-T series	ABIE1C0	Oct 2017
	VMG3925-B10B	AAVF10C0	Dec 2017
	VMG3926-B10A	AAVF10C0	Dec 2017
	VMG5313-B10B	V5.13(AAYY.6)	Dec 2017
	VMG8823-B10B	V5.13(ABEJ.2)	Dec 2017
	VMG8823-B30B	V5.13(ABEJ.2)	Dec 2017
	VMG8823-B50B	V5.13(ABEJ.2)	Dec 2017
	VMG8823-B60B	V5.13(ABEJ.2)	Dec 2017
	VMG8924-B10A VMG8324-B10A	AAKL20C0	Jan 2018

Product	Series/Model	Patch firmware version	Availability
	VMG8924-B10D	V5.13(ABGQ.1)	Dec 2017
	VMG8924-B30A	AAPQ14C0	Jan 2018
	VMG8924-B30D	V5.13(ABGP.1)	Jan 2018
	XMG3512-B series	ABDR1C0	Mar 2018
DSL CPE (Gemini)	Gateway 400	6.38.2.10.03	13-Oct 2017
	Speedlink 5501/6501	4.38.2.10.06	13-Oct 2017
	Speedlink 5502	7.39.2.01.00	27-Oct 2017
	VMG5304	8.39.3	27-Oct 2017
	VMG8029	10.39.3	20-Oct 2017
	VMG8546	9.39.3	20-Oct 2017
Ethernet gateway	EMG2306	V1.00(AAJM.5)C0	Dec 2017
	EMG2926	V1.00(AAVK.6)C0	Oct 2017

Product	Series/Model	Patch firmware version	Availability
	EMG3425	V1.00(AAYJ.11)C0	Dec 2017
GPON ONT	PMG5317-T20A	V521ABCI4C0	30-Nov 2017
	PMG5317-T20B	V540ABKI1C0	30-Nov 2017
Home router	NBG6515	V1.00(AXS.5)C0	Feb 2018
	NBG6604	V1.00(ABIR.2)C0	Jan 2018
	NBG6617	V1.00(ABCT.6)C0	Dec 2017
	NBG6815	V1.00(ABBP.7)C0	Feb 2018
	NBG6816	V1.00(AAWB.10)C0	Dec 2017
	NBG6817	V1.00(ABCS.8)C0	Jan 2018
LTE CPE	LTE4506-M606	V1.00(ABDO.3)C0	15-Dec 2017
	LTE7410	V2.60(ABAW.6)C0	Feb 2018

Product	Series/Model	Patch firmware version	Availability
	LTE7460	V1.00(ABFR.4)C0	20-Dec 2017
	WAH7706	V1.00(ABBC.8)C0	22-Dec 2017
WiFi system	WSQ50	V1.00(ABKJ.2)C0	10-Nov 2017
Wireless extender	WAP6806	V1.00(ABAL.6)C0	18-Feb 2018

What should I do now to protect against the vulnerabilities?

The following short-term mitigations could be put in place to remove or reduce the threat:

- For ISP customers, ISP's DNS server filters all DNS responses to check for the malicious code
- Zyxel CPE is reconfigured so that it does not act as the DNS server for LAN side DHCP clients by issuing the DNS servers as "obtained from ISP" or DNS static IPs. Note this mitigation is only applicable to VDSL and LTE models.

For more information and technical details regarding the vulnerabilities please see below references:

1. US-CERT VU note: https://www.kb.cert.org/vuls/id/973527
2. Disclosure by Google: https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html

Please contact your local service representatives if you require further information or assistance. To report a vulnerability, please contactsecurity@zyxel.com.tw