ID 112717 FAQ

Multiple Vulnerabilities in DNSMASQ (CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496, CVE-2017-13704, CVE-2015-3294)

Initial Internal Release Date: **11/27/2017**
Initial Release to the public*:* **12/04/2017**
Update Release Date: **11/27/2017**

Summary

DNSMASQ is an open source software which provides network infrastructure and services for small networks, DNS, DHCP, router advertisement and network boot. Ruckus Wireless uses DNSMASQ for its AP and ZD Controller software requirements, primarily to achieve the DHCP and DNS functionality.

Recently, Google has published multiple vulnerabilities in DNSMASQ distribution version 2.77 which can lead to Denial of Service (DoS), Remote code Execution (RCE), Out of Memory (OOM) and Information Leak. The complete list of these vulnerabilities with the details can be found at the below link:
https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html

Ruckus Wireless APs and ZD Controller software currently use version 2.33 of the DNSMASQ software. However, since Ruckus products use this older version of DNSMASQ and also some of the vulnerabilities were either only applicable to version 2.77 or did not impact Ruckus Products due to the way Ruckus Wireless is using the software, Ruckus did an independent analysis of these issues in all the products to ascertain the impact of these listed vulnerabilities Test cases were derived from the reproduction steps provided by Google article and also from the CHANGELOG summary of the DNSMASQ open source official page where the information was given about respective vulnerabilities and fixes. These tests were executed on the Ruckus APs and Zone Director which run version 2.33 of the DNSMASQ.

As part of this exercise, Ruckus product teams were not able to reproduce the issues in the manner described by the reported article(s). However, after inspecting the DNSMASQ versions, it was concluded that Ruckus Wireless's Zone Director Controller and Solo/SZ/Unleashed APs firmware may be potentially impacted by these vulnerabilities that could allow remote attackers to exploit them in ways which may not be known yet.

Hence, Ruckus Wireless has planned to release fixes for these vulnerabilities via software updates as well as provide details about the mitigation(s) and workaround(s) available to reduce or thwart the impact of these vulnerabilities on the Ruckus Products.

ID 112717 FAQ

What are the issues?

Denial of Service attack (DoS): is a type of vulnerability in the DNSMASQ that allows an authenticated and valid user to carry out an attack on the DNSMASQ software by sending new DNS entries to be cached to exhaust the heap buffer to crash the software and effectively render the service unusable.

Remote Code Execution (RCE): is a type of vulnerability in the DNSMASQ that allows an authenticated and valid user to who takes control of the DNS server to send crafted DNS query responses to the AP and controller software to execute arbitrary code on these.

For instance, the attacker after taking control of the DNS server could exploit this vulnerability and send crafted DNS response to AP and controller to append arbitrary code or commands to some of values passed to the system which may lead to undesired results.

Out of Memory (OOM): is a type of vulnerability in DNSMASQ when run with command line options "--add-mac, --add-cpe-id or --add-subnet" `that` can lead to code flow where the memory allocated is not freed and continuously increasing lead to calling the classic OOM caller of the operating system.

Information Leak: is a type of vulnerability in DNSMASQ when running as DHCPv6 server could leak information bypassing the ASLR which can finally lead to RCE.

Note: The details of mechanisms of conducting these attacks are exhibited and discussed in the link provided above.

These vulnerabilities are assigned the CVE IDs and details of the same are explained as below:

SNo.	CVE-ID	CVE Description
1	CVE-2017-14491	DNSMASQ versions up to 2.77 are prone to heap overflow leading to DoS and RCE via crafted DNS response.
2	CVE-2017-14492	DNSMASQ versions up to 2.77 are prone to heap overflow leading to DoS and RCE via crafted IPv6 Router Advertisement Request.
3	CVE-2017-14493	DNSMASQ versions up to 2.77 are prone to heap overflow leading to DoS and RCE via crafted DHCPv6 Request.
4	CVE-2017-14494	DNSMASQ versions up to 2.77 when configured as relay allows attackers obtain memory information via forwarded DHCPv6 Requests.
5	CVE-2017-14495	DNSMASQ versions up to 2.77 when used with -add-mac, -add-cpe-id or add-subnet options are prone to DoS attack via crafted DNS response.
6	CVE-2017-14496	DNSMASQ versions up to 2.77 when used with -add-mac, -add-cpe-id or add-subnet options are prone to DoS attack via crafted DNS request, because of Integer underflow.
7	CVE-2017-13704	DNSMASQ versions up to 2.77 may crash this service if the DNS packet size is negative and the software tries to access memory that it beyond its jurisdiction.

8	CVE-2015-3294	DNSMASQ versions prior to 2.73rc4 improper error handling are prone to remote attackers reading process memory and cause DoS via a malformed DNS Request.

How do these vulnerabilities impact Ruckus products?

Although DNSMASQ software is present on multiple Ruckus products, its usage and the impacts of the vulnerabilities vary on each product, as described below.

a) **SCI:** DNSMASQ package is present on the SCI system, but it is not in use. Since there is no impact of the DNSMASQ on SCI product the DNSMASQ package will be removed in upcoming SCI 3.5 GA scheduled for Nov 2017.

b) **SPoT:** DNSMASQ package is present on SPoT, but it is not in use. No impact on SPoT. There is no release scheduled for SPoT, however, as best practice, next maintenance release for SPoT, the DNSMASQ package will be removed.

c) **SZ-300:** DNSMASQ package is present on the SZ-300 system, but it is not in used as daemon but as package dependency. Since there is no impact on SZ-300, but the package needs to be present on the system as dependency, hence, as best practice DNSMASQ package will be upgraded to version 2.78 in SZ-3.6 GA scheduled for Nov 2017.

d) **Solo AP:** Out of 8 vulnerabilities listed, solo AP may potentially be affected by 2 issues. Also, since mitigation/workaround exist, the impact on solo APs, is categorized as low impact. However, as a best practice, affected vulnerabilities shall be fixed in current version 2.33 of DNSMASQ package in version 108 GA scheduled for Nov 2017. Due to low impact, mitigation/workaround is sufficient for the all the previous solo AP releases. In all the future scheduled versions above 108.1, DNSMASQ package will be upgraded to version 2.78.

e) **SZ AP:** Out of 8 vulnerabilities, SZ AP may potentially affected by 2 issues**.** Also, since mitigation/workaround exist, the impact on solo APs, is categorized as low impact. However, as a best practice, affected vulnerabilities shall be fixed in current version 2.33 of DNSMASQ package in R3.6 GA scheduled for Nov 2017.

f) **Unleashed:** Medium Impact is assessed on Unleashed APs as Ruckus Product teams were not able to successfully reproduce the issues in version 2.33 of the DNSMASQ as per the reproduction steps and PoC scripts provided by Google. However, affected vulnerabilities shall be fixed in current version 2.33 of DNSMASQ package in Unleashed 200.6 GA scheduled for April 2018 and also all the MR releases for Unleashed APs for active branches. Any future release of Unleashed 200.6.1+ shall contain latest version 2.78 of DNSMASQ package with fixes.

g) **Zone Director:** Medium Impact on Zone Director as we were not able to successfully reproduce the issues in version 2.33 of DNSMASQ as per the reproduction steps and PoC scripts provided by Google. However, affected vulnerabilities shall be fixed in current version 2.33 of DNSMASQ package in ZD 10.1 GA scheduled for Dec 2017 and also all the MR releases for Zone Director for active branches. Any future release of ZD 10.1.1+ shall contain latest version 2.78 of DNSMASQ package with fixes.

Below table provides the details of the area of impact of each CVE and affected Ruckus products:

ID 112717 FAQ

Sno	CVE-ID	Impacted Area	Affected Ruckus Products	Comments
1	CVE-2017-14491	DNS	**Affected:** Following products and versions may be potentially impacted: solo AP – 104.0 and above. SZ AP- R3.5.0 and above Unleashed APs – All versions of Unleashed APs, where local DHCP service can be configured. ZD - All versions of Zone Director where local DHCP service can be configured.	**Fixes are planned.**
2	CVE-2017-14492	DHCPv6	Not Affected	The Ruckus Products only use IPv4 and DNS functionality not IPv6 and hence are not impacted.
3	CVE-2017-14493	DHCPv6	Not Affected	The Ruckus Products only use IPv4 and DNS functionality not IPv6 and hence are not impacted.
4	CVE-2017-14494	DHCPv6	Not Affected	The Ruckus Products only use IPv4 and DNS functionality not IPv6 and hence are not impacted.
5	CVE-2017-14495	DNS	Not Affected	The vulnerability is only exploitable when the --add-mac, --add-cpe-id or --add-subnet options are specified while bringing DNSMASQ process. Since Ruckus does not use these command line options while using DNSMASQ, hence Ruckus products are not impacted.
6	CVE-2017-14496	DNS	Not Affected	The vulnerability is only exploitable when the --add-mac, --add-cpe-id or --add-subnet options are specified while bringing DNSMASQ process. Since Ruckus does not use these command line options while using DNSMASQ, hence Ruckus products are not impacted.
7	CVE-2017-13704	DNS	Not Affected	Not impacted as per the comments given by DNSMASQ author Simon Kelly. The issue was introduced during a bug fix in ver2.77 and Ruckus Products use version 2.33.
8	CVE-2015-3294	DNS	**Affected:** Following products and versions may be potentially impacted: solo AP – 104.0 and above. SZ AP- R3.5.0 and above Unleashed APs – All version of Unleashed APs, where local DHCP service can be	This CVE-ID is not part of Google disclosure but included since the CVSS score is 6.4, and as per Ruckus Policy we MUST fix any vulnerability which is >6.0 base score. Scenario is that if the DNS request is malformed and DNSMASQ is running DNS Proxy

			configured. ZD - All versions of Zone Director where local DHCP service can be configured.	functionality then on the receipt of the request it crashes. **Fix is planned.**

Are there any workarounds available?
Following workarounds are available to overcome CVE-2017-14491, CVE-2015-3294:

A. All DNS related vulnerabilities can only be exploited if the DNSMASQ runs in DNS Proxy mode. Hence, to prevent the DNSMASQ from running in the DNS Proxy mode, it is advised that the primary and secondary DNS server configuration MUST be configured, although they are optional. At present only Solo AP and SZ-AP firmware provide mechanism to configure the primary and secondary DNS servers. The Unleashed AP and ZD do not have configuration to input the primary and secondary DNS Server IPs for the DHCP Pools (also known as Local Subnets), hence the workaround mentioned below will not be applicable for the Unleashed and ZD products. The details of the workaround for Solo and SZ AP firmware are mentioned as below:

I. **Solo AP:** Currently in Solo APs, while configuring the DHCP service in the GUI under "Local Subnet", there is no configuration to input the DNS server IP values. However, the DNS server IP configuration can be added/modified via AP CLI. Below are steps which needs to be executed on Solo APs to enable the workaround:

Step 1) Login to AP via SSH using AP IP and input required login and password credentials.

Step 2) Once successfully logged in, the AP CLI prompt will appear as "rkscli:"

Step 3) To add or modify the DNS primary and secondary server configuration use below CLI command with required syntax and parameters.

"set subnet <local subnet name> dnsipaddr [enable | disable] {primaryip secondaryip}"

```
rkscli: set subnet local-subnet1 dnsipaddr enable 8.8.8.8 4.4.4.4
```

Once the AP CLI is successful, DNSMMASQ daemon is restarted automatically and the configuration is updated.

Step 4) To verify that the DNS IPs are configured correctly, use "get subnet" CLI command to view the output

```
rkscli: get subnet local-subnet1
```

The output of the get subnet command, will contain the primary and secondary DNS Server IP values as shown below:

```
Primary Dnsip           : 8.8.8.8
Secondary Dnsip         : 4.4.4.4
```

II. **SZ-AP:** For the APs managed via SZ controller the DNS Server Configuration is part of the SZ UI and can easily be configured as mentioned in the steps below:

Step 1) Login to SZ Web UI using the SZ Management IP address via Web browser and input login and password credentials.

Step 2) After successful login, navigate by clicking on “Services & Profiles” and then click on service “DHCP & NAT”.

Step 3) Click on tab “DHCP Pools(AP)” on right side of the pane and select the pool from the list for which the DNS IP addresses are required to be configured.

Step 4) Click on Configure field which will open window “Edit DHCP Pool <Pool Name>”.

Step 5) Click on text field configuration “Primary DNS IP” and input appropriate DNS IP address value (e.g. 8.8.8.8), if the field is blank.

Step 6) Click on text field configuration “Secondary DNS IP” and input appropriate DNS IP address value (e.g. 4.4.4.4), if the field is blank

Step 7) Click on “OK” Button. Verify the configured IP addresses show up in the DHCP Pool table against the Pool configured.

Note:

- If there are multiple local subnets configured on Solo AP, then above-mentioned steps need to be repeated for all the configured local subnets.
- If there are multiple DHCP Pool Profiles in the Zone, then above-mentioned steps need to be repeated for all the configured DHCP Pool profiles.
- The primary and secondary DNS IP addresses mentioned above are for illustration purpose only. Provide the IP address value in the text fields applicable to network configuration.
- Please refer the admin guide of the SZ releases which also contains detailed steps to configure the DHCP pools.

B. CVE-2017-14491 particularly can only be exploited if the attacker takes control of the external DNS server running in the network and start sending the crafted DNS response to Ruckus AP, Unleashed AP or Zone Director. Hence to avoid this it is highly advised that the Ruckus APs / Controller and the DNS server should be secured in such a manner that attacker cannot take control of the DNS server.

What releases fixes are available?

Platform	Release*	Target Patch Release Date
SCI	3.5	Nov 2017
SPoT	Next maintenance release	Not Planned yet. But the DNSMASQ package shall be removed in the next MR.
SZ-300	3.6	Nov 2017
Solo AP	108	Nov 2017
SZ AP	3.6	Nov 2017
Unleashed	200.6	Apr 2018
Zone Director	10.1.0 10.0.1.0 9.13.3.0	Dec 2017 Jan 2018 Dec 2018

ID 112717 FAQ

How does Ruckus Wireless qualify severity of security issues?

Ruckus Wireless typically utilizes the Common Vulnerability Scoring System (CVSS) v3. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. In cases where CVSS v3 scores are not available, CVSS v2 score are provided. Below are the CVSS scores and vector information for respective CVEs:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2017-14491	9.8 (Critical)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2017-14492	9.8 (Critical)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2017-14493	9.8 (Critical)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2017-14494	5.9 (Medium)	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2017-14495	7.5 (High)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2017-14496	7.5 (High)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2017-13704	7.5 (High)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2015-3294	6.4 (Medium)	(AV:N/AC:L/Au:N/C:P/I:N/A:P)

When will this Ruckus Wireless Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: **11/27/2017**

Ruckus Wireless released the initial security advisory to customers on: **12/04/2017**

Public posting: **12/04/2017**

Revision History

ID	Change	Date
112717	Initial Publication to Ruckus Field Teams	November 27, 2017

Ruckus Support can be contacted as follows:

The full contact list is at: https://support.ruckuswireless.com/contact-us

DISCLAIMER