Product Support Notice

PSN #	PSN004238u

Original publication date: 26-Jun-14. This is Issue #01, published date: 26-Jun-14.

Severity/risk level: High

Urgency: When convenient

Name of problem

Malformed DHCP packets are discarded by Stackable Ethernet Routing Switches (ERS) when DHCP snooping, DHCP relay or NonEap Phone Authentication using DHCP signature is enabled on the switches.

Products affected

Ethernet Routing Switch 2500 Series
Ethernet Routing Switch 3500 Series
Ethernet Routing Switch 4000 Series
Ethernet Routing Switch 5000 Series
VSP 7000 Series

Problem description

In some releases of the Stackable ERS platforms (ERS 2500, 3500, 4000 and 5000 Series) as well as the VSP 7000, a software issue was found to cause malformed DHCP packets as they were forwarded out of the switch. When this issue was encountered an extra 4 bytes was added to the payload of the forwarded DHCP packet, but the Total Length in the IP Header was not updated. The resulting malformed DHCP packet is still successfully forwarded or relayed to the next hop toward the DHCP server(s).

In affected releases, these malformed DHCP packets can be generated when any of the DHCP features below is enabled on the switch

- DHCP snooping
- DHCP relay
- NonEap Phone Authentication using DHCP signature (also known as the MultiHostAllowNonEapPhone feature)

A software change which removes the extra 4 bytes in the payload is available in the software versions listed in the Resolution section of this PSN. Due to the nature of this fix, there are potential interaction scenarios between code versions which will need to be managed within the context of a network upgrade to releases containing the code changes.

As part of the fix to eliminate the malformed DHCP issue in newer software versions, a software check was included to detect and discard any malformed DHCP packets which might be received. As the result, there is a potential interaction between affected ERS/VSP switches running different software versions, leading to DHCP packets being dropped and the DHCP clients failing to obtain IP addresses.

The possibility of impact to DHCP packet forwarding exists when a software upgrade is performed in the network. A typical scenario involves core ERS switches with DHCP relay and/or DHCP snooping configured situated in the data path between clients on subtending switches and the DHCP server(s). In such a topology, upgrading the core switches first to the newer software versions while the edge ERS switches hosting DHCP clients remain at older software versions with the DHCP malformed issue will result in DHCP packets being dropped during processing on the upgraded switch.

Resolution

Software versions containing the fix for the malformed DHCP issue are:

- ERS 25xx: >= 4.4.3. Note: ERS 25xx is in End of Sales and currently there is no schedule planned for 4.4.3 software version.

- ERS 35xx: >= 5.1.2, >= 5.2.x

- ERS 4xxx: >= 5.6.4, >=5.7.1, >= 5.8.x

- ERS 5xxx: >=6.2.8, >=6.3.3, >=6.6.x

- VSP 7xxx: >= 10.3.2, >= 10.4.x

If DHCP snooping and/or NonEap Phone Authentication using DHCP signature and/or DHCP relay are used in the network on switches running software versions below those in the table above, it is strongly recommended to upgrade ALL ERS switches along the path to the DHCP server(s) to the latest software versions containing the fix for the malformed DHCP issue. The network upgrade implementation strategy should include consideration of DHCP packet forwarding requirements within the topology and with preference given to upgrading affected ERS switches closest to the client devices first and then progressing towards the core.

Workaround or alternative remediation

If an upgrade strategy that avoids the interaction scenario described above is not feasible, alternative interim solutions may be feasible in some network topologies.

1) Disabling the DHCP features (DHCP snooping, DHCP relay or DHCP signature authentication) on switches running the older software versions so that the malformed DHCP packets are not being generated. Implementation of this option is dependent on the network topology that still allows DHCP packets to reach the DHCP server and may require additional configuration changes.
2) Disabling DHCP snooping and/or DHCP relay on switches running newer software will prevent malformed DHCP packets received from other switches that have not yet been upgraded from being dropped. Implementation of this option may also require additional configuration changes to ensure that the DHCP requests reach the DHCP server.

Remarks

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

Service-interrupting?

n/a

No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686