Date: January 19th, 2021

Version: 1.0

Revision	Date	Changes
1.0	January 19th, 2021	Initial Release
1.1	July 29th, 2021	Updates to fixed versions

The CVE-IDs tracking this issue are: CVE-2020-25684, CVE-2020-25685, CVE-2020-25686

CVSSv3.1 scores and vectors are as follows:

- CVE-2020-25684: 4.0 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N
- CVE-2020-25685: 4.0 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N
- CVE-2020-25686: 4.0 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N

Description

This advisory documents the impact of a vulnerability in Arista's EOS software. Affected software releases are listed below.

Various issues with dnsmasq may result in the dns cache being poisoned by a malicious attacker. The impact is that other clients querying the EOS switch as a DNS server would receive invalid DNS records. This requires an optional configuration to be set in EOS to allow using the EOS switch as a DNS server. This issue may also be known as "DNSPooq" or "ICS-VU-668462" from different sources.

This is an externally found vulnerability and is released as part of a coordinated effort with CERT and dnsmasq.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.25.1F and below releases in the 4.25.x train
- 4.24.3.1M and below releases in the 4.24.x train
- 4.23.6M and below releases in the 4.23.x train
- 4.22.8.1F and below releases in the 4.22.x train
- 4.21.13M and below releases in the 4.21.x train

Affected Platforms

This vulnerability affects all EOS products including the 7xxx and 7xx Series switches and routers, and all CloudEOS packaging options.

The following products are **not affected ***:

- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Wireless Access Points
- CloudVision Wi-Fi (on-premise and cloud service delivery)
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision eXchange, virtual appliance or physical appliance
- CloudVision as-a-Service

* Please note that some Arista products allow customization of native Linux features beyond the scope of typical product usage. We recommend checking these systems to ensure DNS Proxy is not enabled.

Symptoms

In order to be vulnerable, the EOS device must be acting as a DNS server accessible to external devices. This is controlled by the “ip domain proxy” CLI command. This command must be enabled for the device to be vulnerable.

If the device is vulnerable, DNS queries may be altered from their intended upstream values. The only way to determine this is to query for the values using a validation tool and check that they have not been altered from their origin records.

Mitigation

If an EOS upgrade to the remediated version is not feasible, a hotfix patch is available as mitigation against this vulnerability.

The patch can be installed as an EOS extension and is applicable across all affected EOS versions. Installing the patch is briefly disruptive to DNS queries (less than 5 seconds), both externally to the switch and for internal switch services. Installing the patch is non-disruptive to non DNS based control plane traffic and data plane traffic.

For instructions on installation and verification of the hotfix patch, refer to this section in the EOS User Manual: https://www.arista.com/en/um-eos/eos-section-6-6-managing-eos-extensions. Ensure that the patch is made persistent across reboots by running the command ‘copy installed-extensions boot-extensions’.

- Patch file download URL: SecurityAdvisory0061Hotfix.swix
- Sha512sum: f8ddd62583251f9e2863086f188acfd7a729cca4cab91b650ba77b8281e7b353d582cab58ce593f90d4653b356a51aeafe8610e0741bb536b15c634d3f430da0

Resolution

This vulnerability is tracked by Bug 547813. The recommended resolution is to upgrade to a remediated EOS version.

The vulnerability is fixed in the following released versions of EOS - 4.21.14M , 4.22.9M , 4.23.7M , 4.24.5M , 4.25.2F

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request:

Please visit https://www.arista.com/en/support/customer-support for up to date information on how to open a service request via email or telephone.

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25684
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25685
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25686
- https://www.jsof-tech.com/disclosures/dnspooq/
- https://www.thekelleys.org.uk/dnsmasq/CHANGELOG