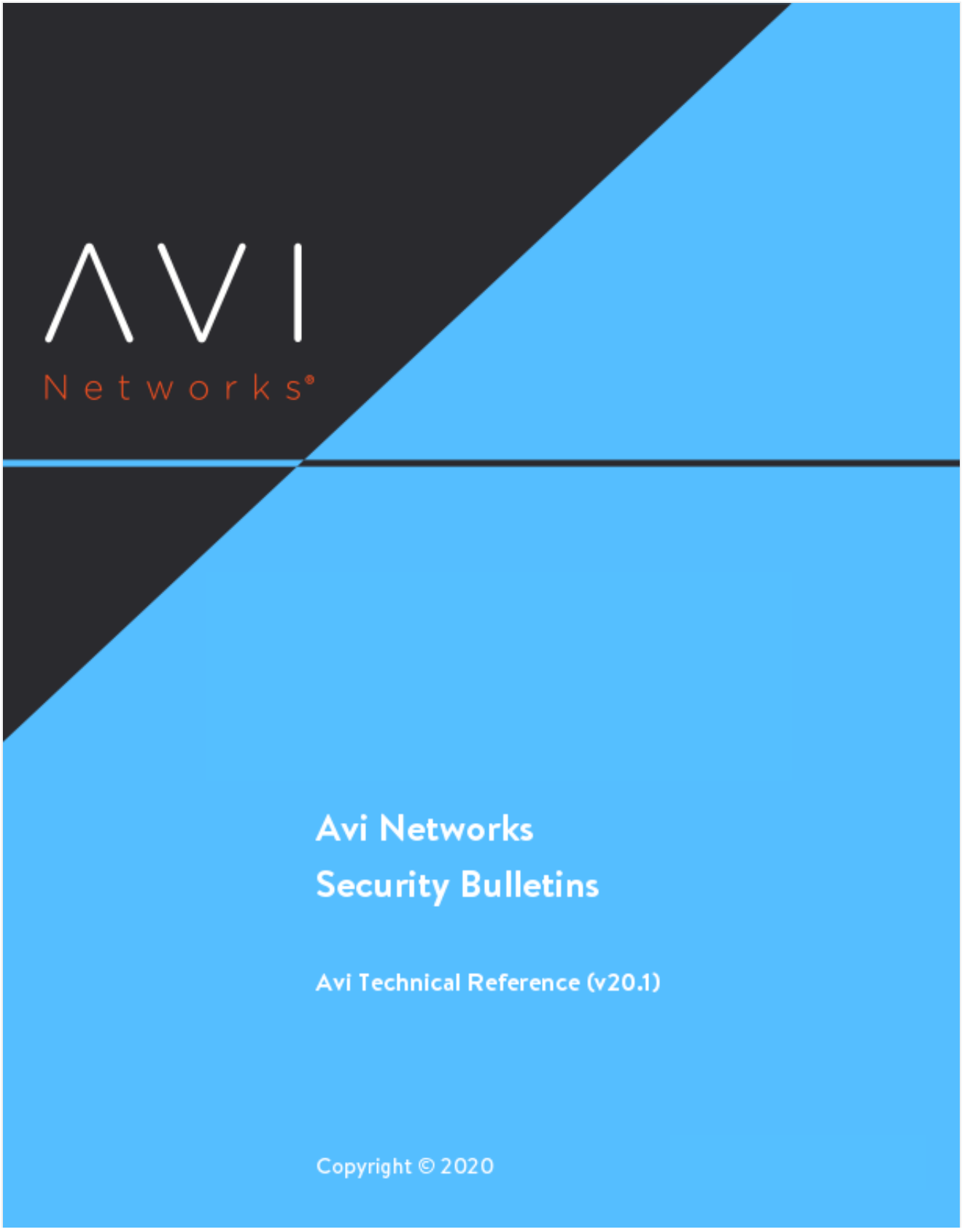

Avi Networks
Security Bulletins

Avi Technical Reference (v20.1)

Avi Networks Security Bulletins

view online

Note

This page has been archived as of October 15, 2020. Going forward, security advisories related to Avi Vantage (now VMware NSX Advanced Load Balancer, NSX ALB) will be available at the VMware Security Advisories page.

See also: Security Advisory Notice (for latest release)

Name	Summary
DoS Vulnerability (CVE-2020-15598) in ModSecurity	Avi Vantage version 17.2.8 and above are not impacted. Avi made changes to the underlying ModSecurity code to avoid performance and potential DoS issues. As part of those changes, the logic in the code base was updated to not do multiple regex matches. This fix was applied to 17.2.8 releases and above. To summarize, the following is the analysis for specific Avi versions: Avi Vantage Version 20.1.x Avi has customised the underlying ModSecurity code over the last few years. Therefore, it is not impacted. Avi Vantage Versions 18.2.x and 17.2.x (17.2.8+) Avi has customised the underlying ModSecurity code over last few years. Therefore, it is not impacted. Avi Vantage version 17.2.x (Pre 17.2.8) Avi versions prior to 17.2.8 may be impacted. Note: As Avi Vantage version 17.2.x is end of support, it is strongly recommended to upgrade to a newer release. Refer to the Upgrade article for more information.

Raccoon Attack in CVE-2020-1968	Avi Vantage is not impacted. Avi Vantage Version 20.1.x Avi Controllers use OpenSSL version 1.0.2g. However, Avi configuration does not allow the use of DH based cipher suites. Hence, the Avi Controller is not affected. Avi Service Engines use OpenSSL versions 1.0.2g as well as base OpenSSL version 1.1.1. • OpenSSL version 1.1.1 is not affected by this vulnerability. • OpenSSL version 1.0.2g: Avi configuration does not allow the use of DH based cipher suites. Hence, the Avi Service Engine is not affected. Avi Vantage Version 18.2.x (18.2.6 and above) Avi Controllers use OpenSSL version 1.0.2g. However, Avi configuration does not allow the use of DH based cipher suites. Hence, the Avi Controller is not affected. Avi Service Engines use OpenSSL versions 1.0.2g as well as base OpenSSL version 1.1.1. • OpenSSL version 1.1.1 is not affected by this vulnerability. • OpenSSL version 1.0.2g: Avi configuration does not allow the use of DH based cipher suites. Hence, the Avi Service Engine is not affected. Avi Vantage Version 18.2.x (18.2.5 and below) Avi Controllers and Service Engines use OpenSSL version 1.0.2g. However, Avi configuration does not allow the use of DH based cipher suites. Hence, the Avi Controller and Service Engine are not affected. Avi Vantage version 17.2.x Avi Controllers and Service Engines use OpenSSL version 1.0.2g. However, Avi configuration does not allow the use of DH based cipher suites. Hence, the Avi Controller and Service Engine are not affected. Note: Avi Vantage version 17.2.x has reached the end of support. Customers are recommended to upgrade to a supported version for continued support and software updates.
Access to Avi Controller file system and system calls via Avi DataScripts	• AV-93265: A valid Avi user with write access to the Avi DataScript role may be able to gain read/write access to the Controller file system, by creating a Protocol Parser script with an invalid filename. Resolution: The vulnerability has been fixed in the following versions of Avi Vantage: ◦ Avi Vantage version 18.2.x: 18.2.10, 18.2.8-2p7, 18.2.9-2p5 ◦ Avi Vantage 20.1.x: 20.1.1-2p3 • AV-92575: A valid Avi user with write access to the Avi DataScript role will be able to execute system commands via Lua functions. Resolution: The vulnerability has been fixed by restricting access to Lua functions available via DataScripts. The vulnerability has been fixed in the following versions of Avi Vantage: ◦ Avi Vantage version 18.2.x: 18.2.10, 18.2.8-2p7, 18.2.9-2p5 ◦ Avi Vantage 20.1.x: 20.1.1-2p3
Segmentation fault in SSL_check_chain - CVE-2020-1967	Avi Vantage is not impacted. Avi Controller uses OpenSSL version 1.0.2g and is not affected by this vulnerability. Avi Service Engine uses OpenSSL version 1.0.2g as well as base OpenSSL version 1.1.1. Both these OpenSSL versions are not affected by this vulnerability.

ROBOT	Avi Vantage is not vulnerable to ROBOT attack, a variant of the Adaptive Chosen CipherText attack, aka Bleichenbacher attack. It targets weak implementations of RSA key exchange protocol.
Meltdown and Spectre	Avi Vantage running in a container or bare-metal environment is not impacted. When Avi Vantage Controller and Service Engine VMs run on Linux, Avi needs to update the kernel for SE and Controller images to include the kernel patches released by the Linux community.

Document Revision History

Date	Change Summary
September 16, 2020	Added the DoS Vulnerability (CVE-2020-15598) in ModSecurity
September 16, 2020	Added the Raccoon Attack in CVE-2020-1968 vulnerability
August 31, 2020	Added DataScripts vulnerability
April 21, 2020	Added OpenSSL vulnerability CVE-2020-1967 -?Segmentation fault in SSL_check_chain"