



Dell SonicWALL Email Security Service Bulletin for Scripting Vulnerability

Dear Customer,

A cross-site scripting vulnerability was reported in the 'License Management' and 'Advanced' pages of Dell SonicWALL Email Security version 7.4.5 that could enable a logged in user to inject malicious code.

Affected Products

- Dell SonicWALL Email Security

Affected Software Versions

- Version 7.4.5 and earlier

Issue Summary

The cross-site scripting vulnerability can occur while uploading patch files on the 'System/Advanced' page or when updating licenses on the "License management" page. Both vulnerabilities can be exploited only when someone with administrative privileges to the email security solution accesses the pages and tries to inject malicious code.

Resolution

We recommend existing users of Dell SonicWALL Email Security upgrade to version 7.4.6 to prevent this cross-site script injection from being executed by unauthorized users. Email Security 7.4.6 is available for download from www.mysonicwall.com. Users should log into mySonicWALL and click on Downloads > Download Center in the navigation panel in the left-hand navigation, then select "Email Security" in the Software Type drop down menu.

Reported by

Benjamin Kunz Mejri

Additional Information

Email Security 7.4.6 release notes is [available here](#).

Please contact Dell SonicWALL Global Support Services www.sonicwall.com/us/support.html