

Service Bulletin: SRA ActiveX Vulnerability

August 19, 2010



Dear Customer

Announcement

E-Class SSL-VPN ActiveX Control format string overflow vulnerability.

Affected Products

SonicWALL Aventail E-Class SRA Products

- EX7000
- EX6000
- EX-2500
- EX-1600
- EX-1500
- EX-750

Affected Software Versions

- 10.0.4 and all previous versions
- 10.5.1 without hot fix

Issue Summary

Remote exploitation of a format string overflow vulnerability in the Endpoint Interrogator/Installer ActiveX Control could allow an attacker to execute arbitrary code within the security context of the targeted user.

Resolution

SonicWALL recommends customers running 10.0.X software upgrade to version 10.0.5 which is available from

Related Information

North America Support:
+1 888.777.1476

International Support:
[Contact](#)

Knowledge Base

[Click Here to Visit the Knowledge Base](#)

www.mysonicwall.com on appliances with an active E-Class Support 24x7 contract. For customers running version 10.5.1 software without the hotfix, please visit our knowledge base to download the 10.5.1 hotfix build: <http://www.sonicwall.com/us/support/kb.asp?kbid=8272>.

Reported by

Nikolas Sotiriou - IT Services

Additional Information

Please contact SonicWALL Global Support Services

www.sonicwall.com/us/support.html

Regards,

SonicWALL Global Support Services

You are receiving this message because you've indicated that you were interested in information from SonicWALL. [Click here to change your email subscription preferences.](#)

© 2010 SonicWALL, INC. | [Privacy Statement](#)
SonicWALL, Inc. Head Offices: 2001 Logic Drive, San Jose, CA 95124-3452, USA