

## Service Bulletin: SRA ActiveX Control Buffer Overflow Vulnerability

October 27, 2010



Dear Kevin

### Announcement

E-Class SRA Service Bulletin for SSL-VPN End Point Interrogator/  
Installer ActiveX Control Buffer OverFlow vulnerability CVE-2010-2583

### Affected Products

SonicWALL Aventail E-Class SRA Products

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

### Affected Software Versions

- 10.0.5 without hotfix "cli-10\_0\_5-003"
- 10.5.1

### Issue Summary

A vulnerability was discovered in SonicWALL E-Class SRA End Point Interrogator/Installer ActiveX Control that can be exploited by malicious hackers to compromise a user's system. This

### Related Information

North America  
Support:  
+1 888.777.1476

International  
Support:  
[Contact](#)

### Knowledge Base

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

vulnerability affects only those customers who are actively using End Point Control.

**Resolution**

SonicWALL recommends customers running 10.5.1 software upgrade to version 10.5.2 which is available from [www.mysonicwall.com](http://www.mysonicwall.com) on appliances with an active E-Class Support 24x7 contract. For customers running version 10.0.X software without hotfix "clt-hotfix-10\_0\_5-003," please visit our Knowledge Base to download the latest 10.0.5 hotfix build: <https://www.fuzeugna.com/sonicwallkb/consumer/kbdetail.asp?kbid=8341..>

**Reported by**

Dmitriy Pletnev, Security Specialist, Secunia

**Additional Information**

Please contact SonicWALL Global Support Services

[www.sonicwall.com/us/support.html](http://www.sonicwall.com/us/support.html)

Regards,

SonicWALL Global Support Services