| | |
|---|---|
| Sense of Security | Authorisation.<br>Jason Edelstein |
| | Release date.<br>30 October 2009. |

**Sense of Security – Security Advisory – SOS-09-008.**

# SafeNet SoftRemote (treename, groupname) Local Buffer Overflow Vulnerability.

30 October 2009.

# SafeNet SoftRemote Local Buffer Overflow - Security Advisory - SOS-09-008

| | |
|---|---|
| **Release Date.** | 30-Oct-2009 |
| **Last Update.** | |
| **Vendor Notification Date.** | 20-Jul-2009 |
| **Product.** | SafeNet SoftRemote |
| **Platform.** | Microsoft Windows |
| **Affected versions.** | 10.8.5 (Build 2), 10.3.5 (Build 6) verified and possibly others<br>Other vendors which have OEM'd the client. |
| **Severity Rating.** | High |
| **Impact.** | System access |
| **Attack Vector.** | Local |
| **Solution Status.** | Fixed in 10.8.9 (unverified) |
| **CVE reference.** | Not currently assigned |

## Details.

SafeNet SoftRemote is an IPsec VPN client that sets up a secure channel for data transport. The application is a popular VPN client which has been OEM'd by many other companies. As a result this vulnerability affects a number of products and vendors.

SafeNet SoftRemote is vulnerable to a local stack based buffer overflow which can lead to the compromise of a vulnerable system.

The vulnerability is caused due to a boundary error when processing certain sections of spd (policy) files. Passing an overly long string to either "TREENAME" or "GROUPNAME" will trigger the overflow.

Successful exploitation results in the execution of arbitrary code.

**Solution.**

Fixed in 10.8.9 (unverified).

**Discovered by.**

Brett Gervasoni from SOS Labs.

**About us.**

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 3, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-09-008

A video demonstrating this exploit can be found at:

http://www.senseofsecurity.com.au/movies/SOS-09-008-safenet.mp4

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php