Sense of Security – Security Advisory – SOS-10-001.

TheGreenBow VPN Client (policy) Local Stack Overflow Vulnerability.

21th January 2010.

TheGreenBow Local Stack Overflow - Security Advisory - SOS-10-001

Release Date.	21-Jan-2010
Last Update.	21-Jan-2010
Vendor Notification Date.	11-Dec-2009
Product.	TheGreenBow VPN Client
Platform.	Microsoft Windows
Affected versions.	4.65.003, 4.51.001 verified and possibly others
Severity Rating.	High
Impact.	System access
Attack Vector.	Local
Solution Status.	Vendor patch
CVE reference.	Not yet assigned

Details.

TheGreenBow is an IPsec VPN client that sets up a secure channel for data transport.

TheGreenBow VPN Client 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 tgb (policy) files. Passing an overly long string to “OpenScriptAfterUp” will trigger the overflow.

Successful exploitation results in the execution of arbitrary code.

Solution.

A patch is available from the vendor (unverified) and will be included in the next release.

Discovered by.

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/consulting/penetration-testing
E: info@senseofsecurity.com.au
Twitter: ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-10-001.pdf

Other Sense of Security advisories can be found at:

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