Advisory Name: Local Privilege Escalation in InterScan Web Security Virtual Apliance 5.0

Internal Cybsec Advisory Id: 2010-0604

Vulnerability Class: Local Privilege Escalation

Release Date: 22-06-2010

Affected Applications: InterScan Web Security Virtual Aplliance 5.0. Other versions may be affected

Affected Platforms: Red Hat nash 5.1

Local / Remote: Local

Severity: Medium - CVSS: 6.8 (AV:L/AC:L/Au:S/C:C/I:C/A:C)

Researcher: Ivan Huertas

Vendor Status: Patched

Reference to Vulnerability Disclosure Policy: http://www.cybsec.com/vulnerability_policy.pdf

Vulnerability Description:

InterScan Web Security Virtual Appliance has a shell called “uihelper” that has suid bit on. So it could be possible to execute commands as root. Also using the vulnerability “Arbitrary File Upload” remote commands could be run as root.

Exploit:

* In order to run commands as root:

$/usr/iwss/AdminUi/uihelper whoami

Impact:

Any user, can escalate privileges and execute arbitrary commands with root user rights.

Solution:

Apply the patch that can be found in

http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=249&regs=NABU&lang_loc=1

Vendor Response:

2009-03-26 – Vulnerability was identified
2010-04-09 – Vendor contacted
2010-04-15 – Vendor response
2010-06-21 – Vendor released fixed version
2010-06-22 – Vulnerability published

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
ihuertas <at> cybsec <dot> com

About CYBSEC S.A. Security Systems

Since 1996 CYBSEC S.A. is devoted exclusively to provide professional services specialized in Computer Security. More than 150 clients around the globe validate our quality and professionalism.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information, please visit www.cybsec.com