CYBSEC®
Security Systems

Advisory Name: Multiple Cross Site Request Forgery vulnerabilities in TP-LINK Admin Panel

Internal Cybsec Advisory Id: 2013-0208-Multiple CSRF vulnerabilities in TP-LINK

Vulnerability Class: Cross Site Request Forgery (CSRF)

Release Date: 02/08/2013

Affected Applications: Firmware v3.13.6 Build 110923 Rel.53137n; other versions may also be affected.

Affected Platforms: WR2543ND or any running the vulnerable firmware.

Local / Remote: Remote

Severity: Medium – CVSS: 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

Researcher: Juan Manuel Garcia

Vendor Status: Acknowedged / Unpatched

Release Mode: User released

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

Vulnerability Description:

Multiple Cross Site Request Forgery vulnerabilities were found in TP-LINK Admin Panel, because the application allows authorized users to perform certain actions via HTTP requests without making proper validity checks to verify the source of the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Proof of Concepts:

1) New Storage Sharing and FTP Server user:
http://tplinklogin.net:80/userRpm/NasUserAdvRpm.htm?nas_admin_pwd=hacker&nas_admin_confirm_pwd=hacker&nas_admin_authority=1&nas_admin_ftp=1&Modify=1&Save=Save

2) Disable the Router's Stateful Inspection Firewall:
http://tplinklogin.net:80/userRpm/BasicSecurityRpm.htm?stat=983040&Save=Save

Impact:

An affected user may unintentionally execute actions written by an attacker. In addition, an attacker may change router settings or gain unauthorized access

Vendor Response:

2012-10-10 – Vulnerability is identified.
2012-10-11 – Vendor is contacted.
2012-10-12 – Vulnerability details are sent to vendor.
2012-10-17 – Vendor confirms vulnerability and states “This vulnerability has been escalated to our RD engineer but under current web server framework it is hard to fix. Our engineer team will modify the web server framework to fix this. Currently it is under process but will take time”.
2012-10-25 – Cybsec asks the vendor for the planned publication date for the update.
2012-10-26 – Vendor states “I have no detailed schedule yet”.
2012-12-12 – Cybsec asks if there are any news regarding the solution of reported vulnerabilities.
2012-12-12 – Vendor states “The fix of this reported vulnerability is not included in the last firmware upgrade because the web server framework change is still under development”.
2013-02-01 – Cybsec tells the Vendor that the security advisory will be published on Wednesday February 6.
2013-02-08 – Having received no reply from TP-Link, vulnerability is 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