RBS-2014-006

Topica TOP-788XMP IP Camera Multiple Actions CSRF and User Creation Security Bypass

Table of Contents

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established in early 2011 to better support the many users and initiatives of the Open Security Foundation - including the OSVDB and DataLossDB projects. RBS was created to transform this wealth of security data into actionable information by enhancing the research available, and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database. Available as feature-rich SaaS portal or powerful API

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.

Vulnerable Program Details

Details for the tested product and version:

Vendor:	TOPICA Technology Co., Ltd.
Product:	TOP-788XMP IP Camera
Version:	3.2.0.6

NOTE: Other models and versions may very likely also be affected.

References

RBS:	RBS-2014-006
OSVDB / VulnDB:	116196[1] and 116197[2]
CVE:	N/A

Credits

Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

[1] http://www.osvdb.org/show/osvdb/116196
[2] http://www.osvdb.org/show/osvdb/116197

Vulnerability Details

Topica TOP-788XMP IP camera provides a web-based interface for viewing the camera feed and configuring device settings. This interface has been determined to be affected by two vulnerabilities.

Cross-Site Request Forgery (CSRF)

HTTP requests to the web-based interface do not require multiple steps, explicit confirmation, or a unique token when performing sensitive actions. By tricking a user into following a specially crafted link, a context-dependent attacker can perform a Cross-Site Request Forgery (CSRF) attack causing the victim to e.g. reboot the device or create administrative users.

The following request reboots the device:
http://[IP]/cgi-bin/reboot.cgi?action=reboot

User Creation Restriction Bypass

The web-based interface supports three types of accounts: “Viewer”, “Remote Viewer”, and “Administrator” with only the third account type permitted to configure the device. For any other account types, access to `user_management_config.html` is restricted i.e. disallowing user management. However, this page just passes entered input to `/cgi-bin/users.cgi` and requests to this CGI script are not restricted to only “Administrator” users.

This allows any authenticated user to submit a POST request to the CGI script to edit existing users or create new users to escalate privileges on the device. Sending the following request would e.g. create an administrative user named “test” with the password “test123”.

action=add&index=5&username=test&password=test123&privilege=1

This vulnerability may also be combined with the CSRF to have any logged-in user regardless of account type unknowingly create an administrative user on the device if viewing a malicious web page.

Solution

The vendor was not responsive, and we are not aware of any available fix for these vulnerabilities.

Timeline

2014/07/28	Vulnerability discovered.
2014/12/09	Emailed vendor to obtain details for security contact.
2014/12/23	OSVDB entry published and details made available on VulnDB[3].
2015/04/29	Publication of this vulnerability report.

[3] https://www.riskbasedsecurity.com/risk-data-analytics/vulnerability-database/