CHECK POINT PROTECTING AGAINST MISFORTUNE COOKIE AND TR-069 ACS VULNERABILITIES

SEVERITY OF RESIDENTIAL GATEWAY (SOHO ROUTER) COMPROMISE

The security of residential gateways is notoriously weak. Between devices running with default admin credentials, old versions of software and zero-to-little patch management in place, the home router security landscape is woefully behind the times.

When an attacker controls a home router, they can affect traffic in subtle ways . Details for two separate gateway-based campaigns were brought to the public eye this year with similar characteristics:

- Massive amount of home routers compromised
- Any user traffic destined for banking or financial sites was redirected to malicious servers under the attackers control or redirected through SSL proxies where the security of the traffic was compromised via an SSL man-in-the-middle attack.

Collections of compromised home routers could be used for large-scale DoS attacks, spam campaigns, attack launch pads and covert eavesdropping on traffic.

MISFORTUNE COOKIE VULNERABILITY

Researchers from Check Point's Malware and Vulnerability Research Group have uncovered a critical vulnerability present on millions of SOHO router and gateway devices. The vulnerability is in an embedded web server installed on millions of customer gateway devices. This web server happens to be used by ISPs to manage Customer Premise Equipment (CPE) via CPE WAN Management Protocol (CWMP). An attacker can use this vulnerability to remotely control CPE gateway devices such as DSL/Cable/FiOS routers with administrative privileges.

The Misfortune Cookie vulnerability is exploitable due to an error within the HTTP cookie management mechanism present in the affected software, allowing an attacker to determine the 'fortune' of a request by manipulating cookies. Attackers can send specially crafted HTTP cookies that exploit the vulnerability to corrupt memory and alter the application state. This, in effect, can trick the attacked web server to treat the current session with administrative privileges.

Research detected at least 12 million readily exploitable devices globally on the Internet. There are no public exploits for Misfortune Cookie but it is possible certain attackers have already discovered and exploited the vulnerability in private, remaining undetected for extensive periods of time. Because of a unique combination of severity, ease of exploitability, and the sheer amount of vulnerable devices, we believe this is a very important issue for users and ISPs.

The affected software is the embedded web server RomPager from AllegroSoft. Internet-wide scans suggest RomPager is likely the most popular web server software in the world with respect to number of available endpoints. RomPager is typically embedded in the firmware released with the device. This specific vulnerability was introduced to the code base in 2002. Vulnerable versions are susceptible to Misfortune Cookie on either port 80 or any CWMP port.

AllegroSoft released a fixed version to address the Misfortune Cookie vulnerability in 2005. However, the patch propagation process is complicated. Due to the way chip manufacturers bundle applications in Software Development Kits for certain chipsets and the way application updates are integrated in router firmware, many devices ship with the vulnerable version in place. Additionally, in order to patch the 12 million vulnerable devices in the wild, manufacturers will have to obtain an updated version of RomPager, integrate it into their current firmware for all vulnerable lines and models, release the firmware version, and then users and/or Internet Service Providers will have to install the update on every vulnerable device in the world. This update may be easier for ISPs by bulk installing via the TR-069 protocol.

Check Point actively contributes to the security community by making independent research progress and working towards better public security awareness and education.

WHAT IS TR-069/CWMP?

TR-069 is a document or specification created by The Broadband Forum that defines the CPE WAN Management Protocol (CWMP). The Broadband Forum consists of key players in the broadband market that define standards and work towards common goals.

CWMP is designed to be a secure architecture in which Customer Premise Equipment (CPE) devices initiate connections to an Auto-Configuration Server (ACS), and accept RPC commands via the XML based Simple Object Access Protocol (SOAP). RPC commands can consist of:

- Set/Get Configuration Parameters
- Receive updates
- Upload/Download files
- Reboot device
- Perform a Factory Reset

CWMP is proving useful, more ISPs are adopting it, and more devices are shipping with it enabled, such as VOIP phones, webcams and set-top cable boxes/DVRs. The default TCP port for CWMP is 7547; research shows this is currently the second most active server port listening on the Internet next to TCP port 80.

ACS VULNERABILITIES

The ability to control one ACS, in-turn, allows an attacker to control many thousands of home routers.

Earlier this year Check Point's Malware and Vulnerability Research Group discovered a number of vulnerabilities in several ACS implementations. The vulnerability types are quite severe consisting of Remote Code Execution, authentication bypass, SQL injection, Denial of Service, and arbitrary file creation. This research highlighted the severity of ACS compromise and alerted ISPs to implement defense-in-depth around their TR-069 deployments.

PROTECTIONS AND MITIGATIONS

Check Point's ThreatCloud Operations Center has released the following IPS Signatures that can be used to prevent Misfortune Cookie and ACS attacks.

Internet Service Providers can set CPE devices to notify when configuration parameters change via the ACS. Parameters that change are reported using the TR-069 Inform RPC. Monitoring for unexpected configuration changes can help providers detect compromised devices. Changes in devices administrator credentials, DNS server, ACS server, and other important settings can indicate compromise. ACS and CPE logs should be monitored for abnormal characteristics.

Network architecture can be examined and, if not already, security devices and controls can be deployed to restrict and monitor TR-069/CWMP traffic. Firewall policies should block this traffic from unexpected IP ranges. Preferably IPS would also be deployed inline to prevent attacks. In the event that a providers network is not architected to allow monitoring for TR-069/CWMP attacks real-time, traffic can be passively monitored for added visibility and attack detection.

A surprising amount of providers use unencrypted communications for CPE management. TR-069 provisioning and connection requests can implement strict TLS (SSL) where the TR-069 client implementation properly validates server certificates to improve overall security.

Disabling additional services on the ACS machine will reduce attack surface. For example running DNS servers and web servers on the ACS increases risk and provides additional points of compromise.

The version and patch level of ACS and CWMP software should be reviewed with hardware vendors to determine if devices or servers are vulnerable. If so work with vendors to deploy server patches and update customer device firmware where appropriate. A patch update policy where patches are regularly applied and reviewed will reduce exposure to vulnerabilities.

A few additional steps can be taken by Internet Service Providers to mitigate risk:

- If possible, use a custom URL path and port for the ACS URL, to avoid automatic detection by opportunistic attackers.
- Using a non-standard port for CWMP can reduce simple scans from discovering CWMP devices automatically and disrupt opportunistic attacker exploitation.
- Reconfiguring CWMP networks to use private non-routable internet addresses will prevent off-network attacks.
- Blocking CWMP port access from outside the network will also prevent off-network attacks.
- Enable authentication for all requests, including connection requests.
- If the ACS solution allows it, use a distinct username/password pair for each provisioned device, assigned at the initial provisioning session.
- Disable user tampering of TR-069 client connection settings.
- Enable alarms for any ACS authentication failure.
- Enable rate blocking for API calls if available.

IPS PROTECTION DETAILS

Protection Name	CVE	Protection Description	Release Date
TR-069 Auto Configuration Servers Multiple Vulnerabilities	CVE-2014-2840 CVE-2014-4956 CVE-2014-4916 CVE-2014-4917 CVE-2014-4918 CVE-2014-4957	The TR-069 protocol allows remote management of end-user broadband devices. Several vulnerabilities have been detected in certain TR-069 server implementations that could allow a remote attacker to obtain administrative access to the servers or execute arbitrary code on them.	28 July 2014
RomPager Authorization Buffer Overflow Denial of Service	CVE-2014-9223	A buffer overflow vulnerability exist in RomPager Web Server. A remote attacker could exploit this vulnerability by sending a crafted request to the vulnerable server causing a denial of service.	21 December 2014
RomPager Authentication Security Bypass – MisfortuneCookie	CVE-2014-9222	An authentication bypass vulnerability exists in RomPager Server. The vulnerability is due to an insecure design in the RomPager Server. Remote attacker could exploit this vulnerability to access the RomPager web-server under administrator privileges.	21 December 2014

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com