Misfortune Cookie Vulnerability

Misfortune Cookie Vulnerability - Check Point Software Technologies, @jifa, Misfortune Cookie Vulnerability by Check Point.

- Published: date not stated
- Original: <https://web.archive.org/web/20160403035045/http://mis.fortunecook.ie/>
- Current location: <https://web.archive.org/web/20160406123152/http://mis.fortunecook.ie/>
- Preserved from: https://web.archive.org/web/20160406123152/http://mis.fortunecook.ie/ (live) on 2026-08-09
- Capture timestamp: 20160403035045
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Misfortune Cookie by Check Point

The Wayback Machine - https://web.archive.org/web/20160406123152/http://mis.fortunecook.ie:80/

[image: image]

What is the Misfortune Cookie vulnerability?

Researchers from Check Point's Malware and Vulnerability Research Group recently uncovered this critical vulnerability present on millions of residential gateway (SOHO router) devices from different models and makers. It has been assigned the CVE-2014-9222 identifier. This severe vulnerability allows an attacker to remotely take over the device with administrative privileges.

How many devices are affected?

To date, researchers have distinctly detected approximately 12 million readily exploitable unique devices connected to the Internet present in 189 countries across the globe, making this one of the most widespread vulnerabilities revealed in recent years. Research suggests the true number of affected devices may be even greater.

How does it affect me?

If your gateway device is vulnerable, then any device connected to your network - including computers, phones, tablets, printers, security cameras, refrigerators, toasters or any other networked device in your home or office network - may have increased risk of compromise. An

attacker exploiting the Misfortune Cookie vulnerability can easily monitor your Internet connection, steal your credentials and personal or business data, attempt to infect your machines with malware, and over-crisp your toast.

Is it that bad?

Yes.

What can I do to protect against the vulnerability?

First of all, be smart about your privacy. Make sure your devices and any documents or folders containing sensitive information are password protected. Consider adding more privacy to your browsing by using HTTPS connections to encrypt all your browser activity.

Watch for firmware updates from your device vendor addressing Misfortune Cookie, apply the update as it is released.

More technical users may flash alternative firmware to their device, replacing the vulnerable service (note this may void the warranty by your vendor). Another option would be configuring your current gateway as a bridge and using a second secure device as your Internet dialer/gateway.

Check Point IPS does block any attempt to exploit Misfortune Cookie if deployed over live relevant traffic. If you are a service provider in control of device fleets, please read our 'Protecting against Misfortune Cookie and TR-069 ACS Vulnerabilities' whitepaper. If you have a vulnerable device owned and managed by your service provider, you can contact your customer support with the request to fix.

Remember that your router's security is another layer in your network security defenses – you should have endpoint protections in place, including firewalls, anti-virus software, and a freshly updated operating system. Consumers and small- to mid-sized businesses who are interested can visit ZoneAlarm to learn about endpoint protection.

What makes Misfortune Cookie more dangerous than many other embedded device vulnerabilities?

Misfortune Cookie is unique due to a combination of multiple factors, including its severity, ease of exploitability, lacking of almost any preconditions, and the sheer volume of vulnerable networks. In certain countries, we have measured eye-opening vulnerability rates of anywhere between 10% to an estimated 50% of used IP addresses in that country (this is not a typo, 1 in 2 Internet users in these countries is likely vulnerable).

All an attacker needs in order to exploit Misfortune Cookie is to send a single packet to your public IP address. No hacking tools required, just a simple modern browser.

This should be considered an alarming wake-up call for the embedded device industry and consumers alike, highlighting the importance of increased security and privacy for consumer and enterprise networks.

Why have you named it Misfortune Cookie?

The Misfortune Cookie vulnerability is 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 and system state. This, in effect, can trick the attacked device to treat the current session with administrative privileges - to the misfortune of the device owner.

What software component is vulnerable?

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.

Which devices are affected?

Our research has detected at least 200 different models of devices of various manufacturers and brands currently exposing a vulnerable service on the public Internet address space. The majority of these devices are residential gateways. The list includes models by ASUS, D-Link, Edimax, Huawei, TP-Link, ZTE, and ZyXEL, among others. We suspect that the source for inclusion of the vulnerable piece of software is a common chipset SDK (distributed to the different manufacturers), however this cannot be confirmed at this point.

Prior to this publication and the expected firmware patches, we believe that devices exposing RomPager services with versions before 4.34 (and specifically 4.07) are vulnerable. Note that some vendor firmware updates may patch RomPager to fix Misfortune Cookie without changing the displayed version number, invalidating this as an indicator of vulnerability.

Which countries are affected?

We processed scan data to provide an approximate geographical breakdown of affected countries. The measured exposure rate is assigned on a scale of 1 (good) to 5 (bad) where 1 means low numbers of vulnerable endpoints detected and 5 designates critical exposure (a significant percentage of that country's used IP address space identified as vulnerable). This data is known to be partial due to our limited collection method. Our measurement is based on scans of ports 80 and 7547 only. If ISPs in a certain country use different ports for TR-069 (we know for a fact some providers do), they will not show as exposed in this graphic, while they may be vastly vulnerable.

Can I detect if I was compromised using Misfortune Cookie?

Typically you would not have logs or other traces of Misfortune Cookie exploitation. General warning signs may be the inability to log in to the web interface or the discovery of changed settings in your device.

Are any Check Point devices affected by Misfortune Cookie?

No.

Can you further explain the technical risk?

An attacker with administrative access to your gateway holds an alarming control over your wired and/or wireless network (local area network, a.k.a. LAN) infrastructure. Such control puts devices at risk of Man-in-The-Middle attacks, greatly increases the attack surface for LAN-side vulnerabilities, and gives attackers the ability to directly monitor connections and identifiers belonging to your devices.

The implications of these risks mean more than just a privacy violation – they also set the stage for further attacks, such as installing malware on devices and making permanent configuration changes. This WAN-to-LAN free-crossing is also bypassing any firewall or isolation functionality previously provided by your gateway and breaks common threat models. For example, an attacker can try to access your home webcam (potentially using default credentials) or extract data from your business NAS backup drive.

Are you aware of attackers exploiting Misfortune Cookie?

Not yet, although we can assume certain attackers have already discovered and exploited the vulnerability. It can possibly explain some SOHO router attacks we have seen in recent years, though we have no direct evidence yet.

Has it been fixed?

Technically, yes; but it's complicated. AllegroSoft issued a fixed version to address the Misfortune Cookie vulnerability in 2005, which was provided to licensed manufacturers. The patch propagation cycle, however, is incredibly slow (sometimes non-existent) with these types of devices. We can confirm many devices today still ship with the vulnerable version in place. We believe this is a serious problem that the industry needs to solve; secure automatic software updates should be offered for all modern devices, if not as a default setting.

What needs to happen for a patch to arrive at my device?

Generally, all vulnerable device makers need to obtain an updated version of RomPager or patch it manually, integrate the fixed version into their current firmware for all vulnerable lines and models, test that nothing was broken during the process, release the firmware version, which would then have to be installed on every vulnerable device in the world.

If your service provider uses TR-069, it may be much easier for them to install the firmware update in bulk.

That patching process sounds unlikely to happen any time soon.

We know. That's why we consider this a serious problem in need of attention.

Can't you just use the vulnerability to patch it everywhere?

While theoretically that might be possible, performing such pervasive action on devices that are not in your possession would constitute a criminal charge in many countries, regardless of the well intention of the originator.

Why is Check Point performing this type of research?

Since ancient history to modern day, it was proven that in order to understand the adversary, you must become one. These efforts are a part of what makes Check Point a 21-year leader in an ever-changing security landscape.

Check Point actively contributes to the security community by making independent research progress and working towards better public security awareness and education. We've been doing this for a while now, you may have noticed some of our recent work.

How did you find it?

We reversed the firmware binary and looked for vulnerabilities. Check Point researcher *Lior Oppenheim* independently discovered this vulnerability among several other ones. Later it was clarified that the vulnerability had already been known and fixed during an internal code review by AllegroSoft – but is still a serious hole in many devices. The details of our research and methods will be presented at the 31st CCC conference in Germany later this month.

What other vulnerabilities did you find?

We identified a couple of buffer overflow vulnerabilities that have been assigned the CVE-2014-9223 identifier. While these can also lead to complete compromise of the device given knowledge of the target firmware, we decided to focus our research on the more exploitable Misfortune Cookie vulnerability.

How can I exploit Misfortune Cookie?

Check Point does not share exploitation tools or exploit code as a policy, nor will we give you the detailed instructions for creating one. One can assume, however, that other researchers will independently develop such code eventually. We can only encourage you to use it professionally and responsibly.

Which vendors did you disclose these findings to? What was their response?

We contacted AllegroSoft, as well as several major vendors we could identify as having significant numbers of vulnerable model instances. Responses vary from immediate recognition and following to correctly patch firmware binaries to complete lack of response.

Why disclose at all? Aren't you helping the bad guys?

We gave this a lot of thought. As always with vulnerability disclosure there is a consideration including balances between the values of public awareness/knowledge and the associated risks. In this case, we felt public education was the most critical deciding factor, specifically due to the expected lengthy patching process caused by the popularity of the vulnerable software and the diversity of makers and models. This public awareness may serve as a better incentive for the makers to release updated firmware faster.

What does Misfortune Cookie have to do with TR-069?

We began this research by surveying client-side implementations of TR-069 (CWMP), after noticing the extreme prevalence of endpoints listening on the default CWMP Connection-Request port (7547), second only to HTTP (port 80) listening endpoints. Misfortune Cookie was uncovered during the examination of RomPager - the most popular recognized service on this port.

Is this a problem with the TR-069 protocol specification?

While the proliferation of devices managed by TR-069 is responsible for creating a very large vulnerable client population, Misfortune Cookie is not a vulnerability related to the TR-069/CWMP per se. Misfortune Cookie affects any implementation of a service using the old version of RomPager's HTTP parsing code, on port 80, 8080, 443, 7547, and others.

Is this a problem with the security design of RomPager?

Not at all; AllegroSoft were very responsive and security-aware. We just happened to research an old version of their software due to its popularity. We have no reason to believe it is any better or worse than comparable software in 2002.

Is this an intentionally placed back door?

It doesn't look like one.

I need someone to blame.

That's not even a question.

*Page last updated at *

Media Contact Lindsay Bubbico *Check Point Software Technologies* +1-917-754-3013 press@us.checkpoint.com