Hello 0-Days My Old Friend:

A 2024 Zero-Day Exploitation Analysis

Casey Charrier
James Sadowski
Clement Lecigne
Vlad Stolyarov

Google

Scope

This report describes what Google Threat Intelligence Group (GTIG) knows about zero-day exploitation in 2024. The following content leverages original research conducted by GTIG, combined with breach investigation findings and reporting from reliable open sources, though we cannot independently confirm the reports of every source. Research in this space is dynamic and the numbers may adjust due to the ongoing discovery of past incidents through digital forensic investigations. The numbers presented here reflect our best understanding of current data.

GTIG defines a zero-day as a vulnerability that was maliciously exploited in the wild before a patch was made publicly available. GTIG acknowledges that the trends observed and discussed in this report are based on detected and disclosed zero-days. Our analysis represents exploitation tracked by GTIG but may not reflect all zero-day exploitation.

Table of Contents

Executive Summary

Google Threat Intelligence Group (GTIG) tracked 75 zero-day vulnerabilities exploited in the wild in 2024, a decrease from the number we identified in 2023 (98 vulnerabilities), but still an increase from 2022 (63 vulnerabilities). We divided the reviewed vulnerabilities into two main categories: end-user platforms and products (e.g., mobile devices, operating systems, and browsers) and enterprise-focused technologies, such as security software and appliances. This report discusses how targeted vendors and exploited products drive trends that reflect threat actor goals and shifting exploitation approaches, and then closely examines several examples of zero-day exploitation from 2024 that demonstrate how actors use both historic and novel techniques to exploit vulnerabilities in targeted products.

Vendors continue to drive improvements that make some zero-day exploitation harder, demonstrated by both dwindling numbers across multiple categories and reduced observed attacks against previously popular targets. At the same time, commercial surveillance vendors (CSVs) appear to be increasing their operational security practices, potentially leading to decreased attribution and detection.

We see zero-day exploitation targeting a greater number and wider variety of enterprise-specific technologies, although these technologies still remain a smaller proportion of overall exploitation when compared to end-user technologies. While the historic focus on the exploitation of popular end-user technologies and their users continues, the shift toward increased targeting of enterprise-focused products will require a wider and more diverse set of vendors to increase proactive security measures in order to reduce future zero-day exploitation attempts.

Key Takeaways

ZERO-DAY EXPLOITATION CONTINUES TO GROW GRADUALLY

The 75 zero-day vulnerabilities exploited in 2024 follow a pattern that has emerged over the past four years. While individual year counts have fluctuated, the average trendline indicates that the rate of zero-day exploitation continues to grow at a slow but steady pace.

ENTERPRISE-FOCUSED TECHNOLOGY TARGETING CONTINUES TO EXPAND

GTIG continued to observe an increase in adversary exploitation of enterprise-specific technologies throughout 2024. In 2023, 37% of zero-day vulnerabilities targeted enterprise products. This jumped to 44% in 2024, primarily fueled by the increased exploitation of security and networking software and appliances.

ATTACKERS ARE INCREASING THEIR FOCUS ON SECURITY AND NETWORKING PRODUCTS

Zero-day vulnerabilities in security software and appliances were a high-value target in 2024. We identified 20 security and networking vulnerabilities, which was over 60% of all zero-day exploitation of enterprise technologies. Exploitation of these products, compared to end-user technologies, can more effectively and efficiently lead to extensive system and network compromises, and we anticipate adversaries will continue to increase their focus on these technologies.

VENDORS ARE CHANGING THE GAME

Vendor investments in exploit mitigations are having a clear impact on where threat actors are able to find success. We are seeing notable decreases in zero-day exploitation of some historically popular targets such as browsers and mobile operating systems.

ACTORS CONDUCTING CYBER ESPIONAGE STILL LEAD ATTRIBUTED ZERO-DAY EXPLOITATION

Between government-backed groups and customers of commercial surveillance vendors (CSVs), actors conducting cyber espionage operations accounted for over 50% of the vulnerabilities we could attribute in 2024. People's Republic of China (PRC)-backed groups exploited five zero-days, and customers of CSVs exploited eight, continuing their collective leading role in zero-day exploitation. For the first year ever, we also attributed the exploitation of the same volume of 2024 zero-days (five) to North Korean actors mixing espionage and financially motivated operations as we did to PRC-backed groups.

Looking at the Numbers

GTIG tracked 75 exploited-in-the-wild zero-day vulnerabilities that were disclosed in 2024. This number appears to be consistent with a consolidating upward trend that we have observed over the last four years. After an initial spike in 2021, yearly counts have fluctuated but not returned to the lower numbers we saw in 2021 and prior.

While there are multiple factors involved in discovery of zero-day exploitation, we note that continued improvement and ubiquity of detection capabilities along with more frequent public disclosures have both resulted in larger numbers of detected zero-day exploitation compared to what was observed prior to 2021.

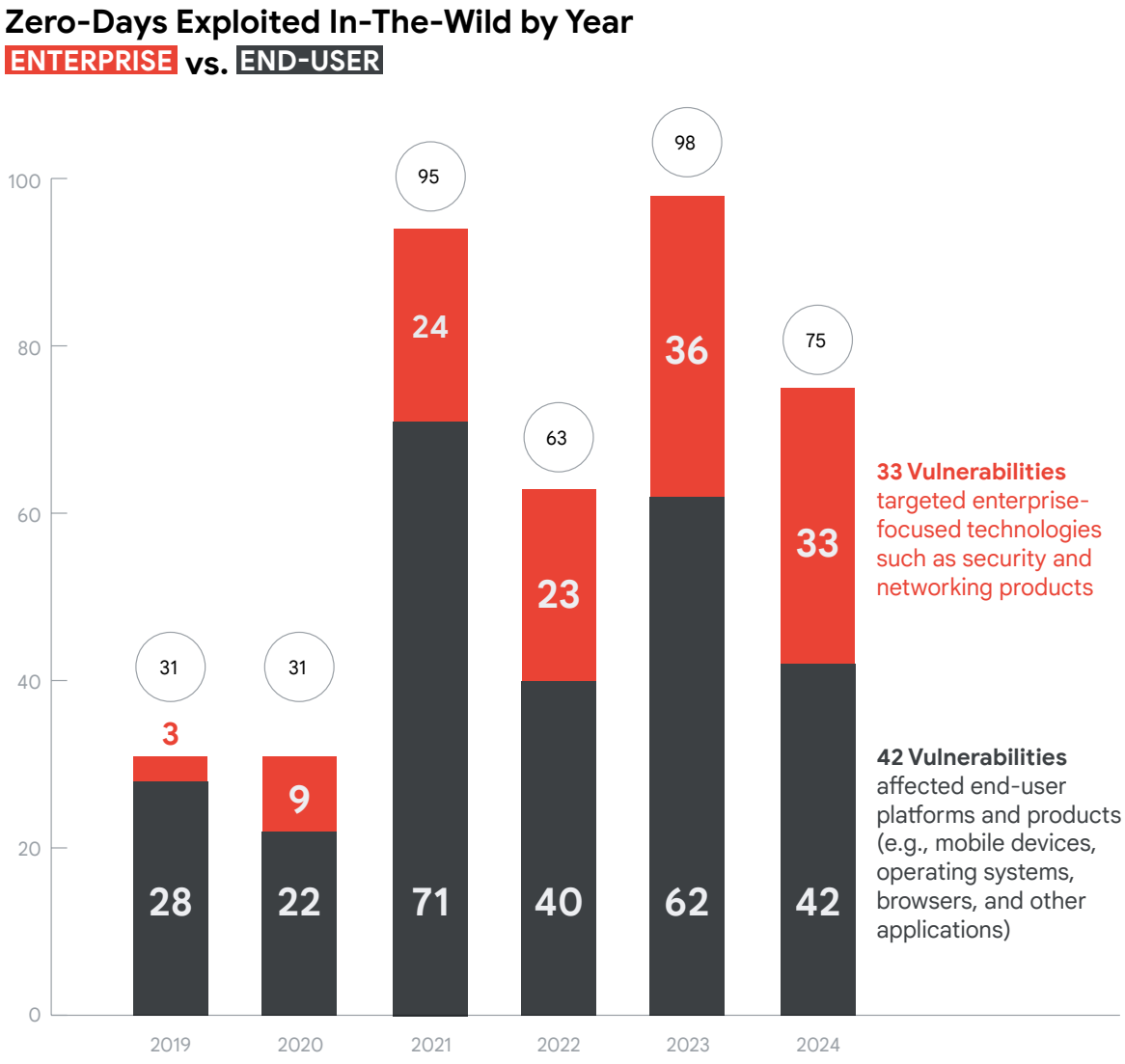
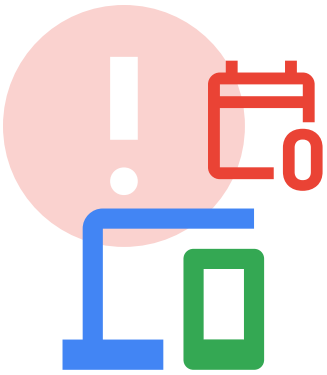


Figure 1: Zero-days by year

Higher than any previous year, 44% (33 vulnerabilities) of tracked 2024 zero-days affected enterprise technologies, continuing the growth and trends we observed last year. The remaining 42 zero-day vulnerabilities targeted end-user technologies.



Enterprise Exploitation Expands in 2024 as Browser and Mobile Exploitation Drops

End-User Platforms and Products

In 2024, 56% (42) of the tracked zero-days targeted end-user platforms and products, which we define as devices and software that individuals use in their day-to-day life, although we acknowledge that enterprises also often use these. All of the vulnerabilities in this category were used to exploit browsers, mobile devices, and desktop operating systems.

- Zero-day exploitation of browsers and mobile devices fell drastically, decreasing by about a third for browsers and by about half for mobile devices compared to what we observed last year (17 to 11 for browsers, and 17 to 9 for mobile).
- Chrome was the primary focus of browser zero-day exploitation in 2024, likely reflecting the browser's popularity among billions of users.
- Exploit chains made up of multiple zero-day vulnerabilities continue to be almost exclusively (~90%) used to target mobile devices.
- Third-party components continue to be exploited in Android devices, a trend we discussed in last year's analysis. In 2023, five of the seven zero-days exploited in Android devices were flaws in third-party components. In 2024, three of the seven zero-days exploited in Android were found in third-party components. Third-party components are likely perceived as lucrative targets for exploit development since they can enable attackers to compromise many different makes and models of devices across the Android ecosystem.
- 2024 saw an increase in the total number of zero-day vulnerabilities affecting desktop operating systems (OSs) (22 in 2024 vs. 17 in 2023), indicating that OSs continue to be a strikingly large target. The proportional increase was even greater, with OS vulnerabilities making up just 17% of total zero-day exploitation in 2023, compared to nearly 30% in 2024.
- Microsoft Windows exploitation continued to increase, climbing from 13 zero-days in 2022, to 16 in 2023, to 22 in 2024. As long as Windows remains a popular choice both in homes and professional settings, we expect that it will remain a popular target for both zero-day and n-day (i.e. a vulnerability exploited after its patch has been released) exploitation by threat actors.

Zero-Day Exploitation of Popular End-User Technologies in 2023 vs. 2024

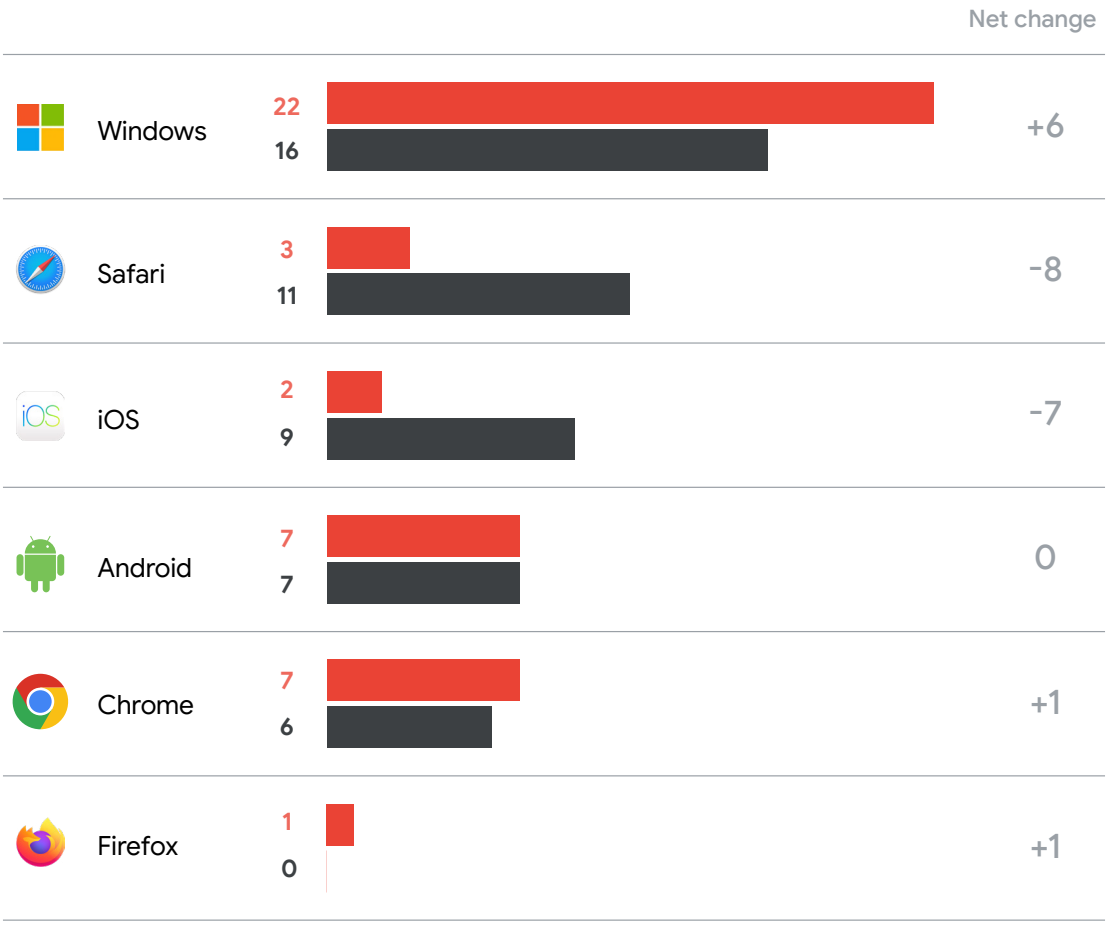


Figure 2: Zero-days in end-user products in 2023 and 2024

Enterprise Technologies

In 2024, GTIG identified the exploitation of 33 zero-days in enterprise software and appliances. We consider enterprise products to include those mainly utilized by businesses or in a business environment. **While the absolute number is slightly lower than what we saw in 2023 (36 vulnerabilities), the proportion of enterprise-focused vulnerabilities has risen from 37% in 2023 to 44% in 2024.** Twenty of the 33 enterprise-focused zero-days targeted security and network products, a slight increase from the 18 observed in this category for 2023, but a 9% bump when compared proportionally to total zero-days for the year.

The variety of targeted enterprise products continues to expand across security and networking products, with notable targets in 2024 including Ivanti Cloud Services Appliance, Palo Alto Networks PAN-OS, Cisco Adaptive Security Appliance, and Ivanti Connect Secure VPN. Security and network tools and devices are designed to connect widespread systems and devices with high permissions required to manage the products and their services, making them highly valuable targets for threat actors seeking efficient access into enterprise networks. Endpoint detection and response (EDR) tools are not usually equipped to work on these products, limiting available capabilities to monitor them. Additionally, exploit chains are not generally required to exploit these systems, giving extensive power to individual vulnerabilities that can single-handedly achieve remote code execution or privilege escalation.

Over the last several years, **we have also tracked a general increase of enterprise vendors targeted.** In 2024, we identified 18 unique enterprise vendors targeted by zero-days. While this number is slightly less than the 22 observed in 2023, it remains higher than all prior years' counts. It is also a stark increase in the proportion of enterprise vendors for the year, given that the 18 unique enterprise vendors were out of 20 total vendors for 2024. 2024's count is still a significant proportional increase compared to the 22 unique enterprise vendors targeted out of a total of 23 in 2023.

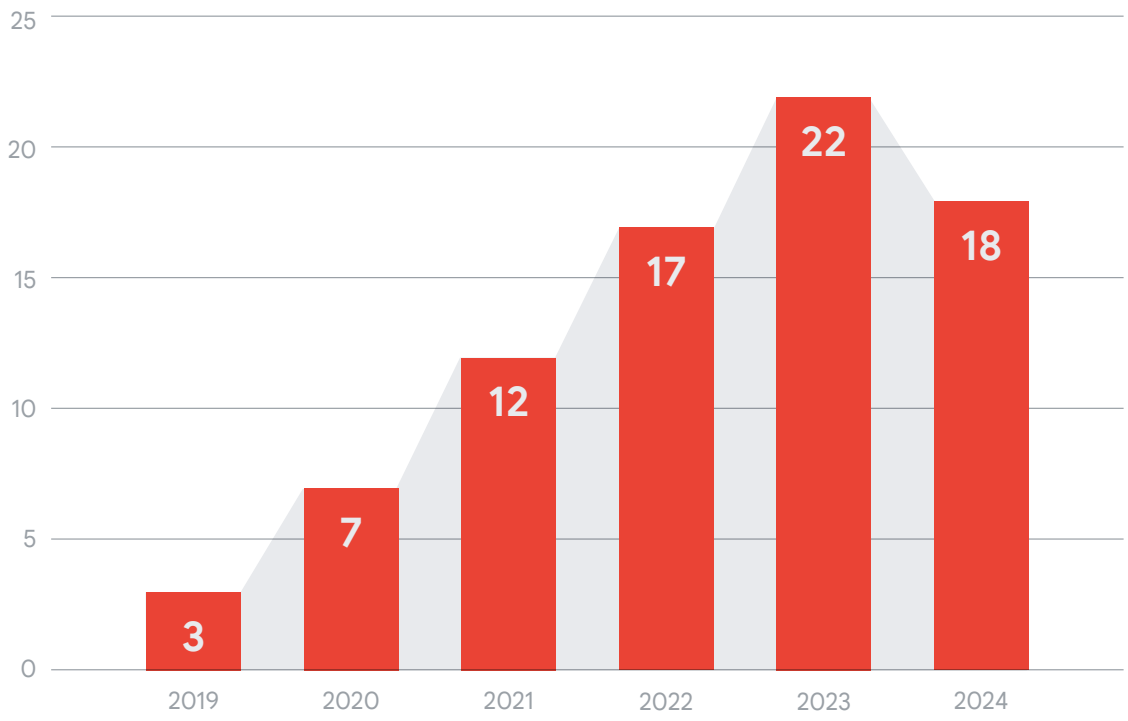


Figure 3: Number of unique enterprise vendors targeted

The proportion of zero-days exploited in enterprise devices in 2024 reinforces a trend that suggests that attackers are intentionally targeting products that can provide expansive access and fewer opportunities for detection.

Exploitation by Vendor

The vendors affected by multiple 2024 zero-day vulnerabilities generally fell into two categories: big tech (Microsoft, Google, and Apple) and vendors who supply security and network-focused products. As expected, big tech took the top two spots, with Microsoft at 26 and Google at 11. Apple slid to the fourth most frequently exploited vendor this year, with detected exploitation of only five zero-days. Ivanti was third most frequently targeted with seven zero-days, reflecting increased threat actor focus on networking and security products. We discuss in a following section how PRC-backed exploitation has focused heavily on security and network technologies, one of the contributing factors to the rise in Ivanti targeting.

This is a new and notable change, where a security vendor was targeted more frequently than a popular consumer technology-focused vendor.

We note that exploitation is not necessarily reflective of a vendor's security posture or software development processes, as targeted vendors and products depend on threat actor objectives and capabilities.

Types of Exploited Vulnerabilities

Threat actors continued to utilize zero-day vulnerabilities primarily for the purposes of gaining remote code execution and elevating privileges. In 2024, these consequences accounted for over half (42) of total tracked zero-day exploitation.

Three vulnerability types were most frequently exploited. Use-after-free vulnerabilities have maintained their prevalence over many years, with eight in 2024, and are found in a variety of targets including hardware, low-level software, operating systems, and browsers. Command injection (also at eight, including OS command injection) and cross-site scripting (XSS) (six) vulnerabilities were also frequently exploited in 2024. Both code injection and command injection vulnerabilities were observed almost entirely targeting networking and security software and appliances, displaying the intent to use these vulnerabilities in order to gain control over larger systems and networks. The XSS vulnerabilities were used to target a variety of products, including mail servers, enterprise software, browsers, and an OS.

All three of these vulnerability types stem from software development errors and require meeting higher programming standards in order to prevent them from occurring. Safe and preventative coding practices, including, but not limited to code reviews, updating legacy codebases, and utilizing up-to-date libraries, can appear to hinder production timelines. However, patches prove the potential for these security exposures to be prevented in the first place with proper intention and effort and ultimately reduce the overall effort to properly maintain a product or codebase.

Who's Driving Exploitation

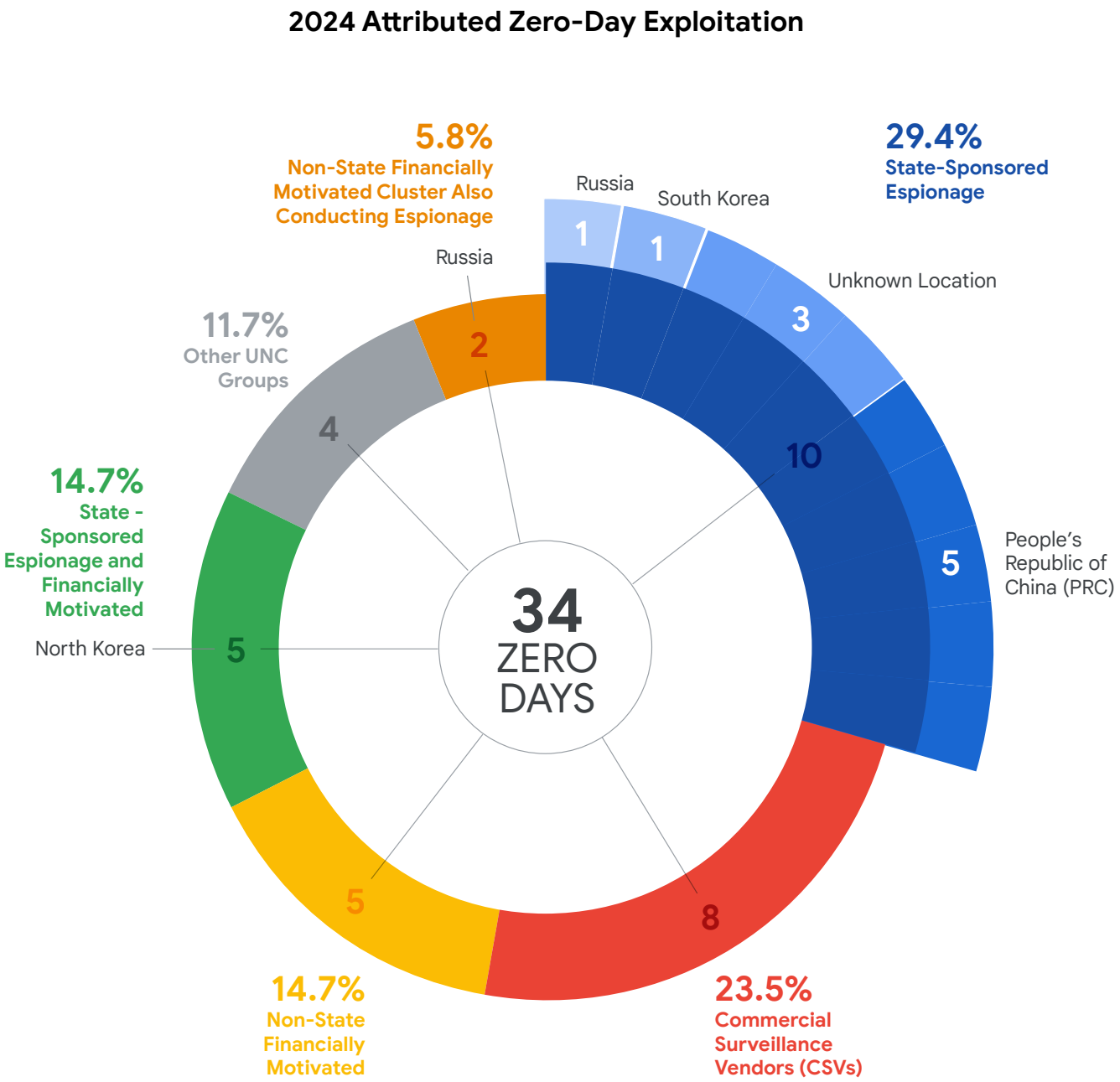


Figure 4: 2024 attributed zero-day exploitation

Due to the stealthy access zero-day vulnerabilities can provide into victim systems and networks, they continue to be a highly sought after capability for threat actors. GTIG tracked a variety of threat actors exploiting zero-days in a variety of products in 2024, which is consistent with our previous observations that zero-day exploitation has diversified in both platforms targeted and actors exploiting them. **We attributed the exploitation of 34 zero-day vulnerabilities in 2024, just under half of the total 75 we identified in 2024.** While the proportion of exploitation that we could attribute to a threat actor dipped slightly from our analysis of zero-days in 2023, it is still significantly higher than the ~30% we attributed in 2022. While this reinforces our previous observation that platforms' investment in exploit mitigations are making zero-days harder to exploit, the security community is also slowly improving our ability to identify that activity and attribute it to threat actors.

Consistent with trends observed in previous years, we attributed the highest volume of zero-day exploitation to traditional espionage actors, nearly 53% (18 vulnerabilities) of total attributed exploitation. Of these 18, we attributed the exploitation of 10 zero-days to likely nation-state-sponsored threat groups and eight to CSVs.

CSVs Continue to Increase Access to Zero-Day Exploitation

While we still expect government-backed actors to continue their historic role as major players in zero-day exploitation, CSVs now contribute a significant volume of zero-day exploitation. Although the total count and proportion of zero-days attributed to CSVs declined from 2023 to 2024, likely in part due to their increased emphasis on operational security practices, the 2024 count is still substantially higher than the count from 2022 and years prior. Their role further demonstrates the expansion of the landscape and the increased access to zero-day exploitation that these vendors now provide other actors.

In 2024, we observed multiple exploitation chains using zero-days developed by forensic vendors that required physical access to a device (CVE-2024-53104, CVE-2024-32896, CVE-2024-29745, CVE-2024-29748). These bugs allow attackers to unlock the targeted mobile device with custom malicious USB devices. For instance, GTIG and Amnesty International's Security Lab discovered and reported on CVE-2024-53104 in exploit chains developed by forensic company Cellebrite and used against the Android phone of a Serbian student and activist by Serbian security services. GTIG worked with Android to patch these vulnerabilities in the February 2025 Android security bulletin.

PRC-Backed Exploitation Remains Persistent

PRC threat groups remained the most consistent government-backed espionage developer and user of zero-days in 2024. **We attributed nearly 30% (five vulnerabilities) of traditional espionage zero-day exploitation to PRC groups**, including the exploitation of zero-day vulnerabilities in Ivanti appliances by UNC5221 (CVE-2023-46805 and CVE-2024-21887), which GTIG reported on extensively. During this campaign, UNC5221 chained multiple zero-day vulnerabilities together, highlighting these actors' willingness to expend resources to achieve their apparent objectives. The exploitation of five vulnerabilities that we attributed to PRC groups exclusively focused on security and networking technologies. This continues a trend that we have observed from PRC groups for several years across all their operations, not just in zero-day exploitation.

North Korean Actors Mix Financially Motivated and Espionage Zero-Day Exploitation

For the first time since we began tracking zero-day exploitation in 2012, in 2024, North Korean state actors tied for the highest total number of attributed zero-days exploited (five vulnerabilities) with PRC-backed groups. North Korean groups are notorious for their overlaps in targeting scope; tactics, techniques, and procedures (TTPs); and tooling that demonstrate how various intrusion sets support the operations of other activity clusters and mix traditional espionage operations with attempts to fund the regime. This focus on zero-day exploitation in 2024 marks a significant increase in these actors' focus on this capability. North Korean threat actors exploited two zero-day vulnerabilities in Chrome as well as three vulnerabilities in Windows products.

- In October 2024, it was publicly reported that APT37 exploited a zero-day vulnerability in Microsoft products. The threat actors reportedly compromised an advertiser to serve malicious advertisements to South Korean users that would trigger zero-click execution of CVE-2024-38178 to deliver malware. Although we have not yet corroborated the group's exploitation of CVE-2024-38178 as reported, we have observed APT37 previously exploit Internet Explorer zero-days to enable malware distribution.
- North Korean threat actors also reportedly exploited a zero-day vulnerability in the Windows AppLocker driver (CVE-2024-21338) in order to gain kernel-level access and turn off security tools. This technique abuses legitimate and trusted but vulnerable already-installed drivers to bypass kernel-level protections and provides threat actors an effective means to bypass and mitigate EDR systems.

Non-State Exploitation

In 2024, we linked almost 15% (five vulnerabilities) of attributed zero-days to non-state financially motivated groups, including a suspected FIN11 cluster's exploitation of a zero-day vulnerability in multiple Cleo managed file transfer products (CVE-2024-55956) to conduct data theft extortion. **This marks the third year of the last four (2021, 2023, and 2024) in which FIN11 or an associated cluster has exploited a zero-day vulnerability in its operations, almost exclusively in file transfer products.** Despite the otherwise varied cast of financially motivated threat actors exploiting zero-days, FIN11 has consistently dedicated the resources and demonstrated the expertise to identify, or acquire, and exploit these vulnerabilities from multiple different vendors.

We attributed an additional two zero-days in 2024 to non-state groups with mixed motivations, conducting financially motivated activity in some operations but espionage in others. Two vulnerabilities (CVE-2024-9680 and CVE-2024-49039, detailed in the next section) were exploited as zero-days by CIGAR (also tracked as UNC4895 or publicly reported as RomCom), a group that has conducted financially motivated operations alongside espionage likely on behalf of the Russian government, based partly on observed highly specific targeting focused on Ukrainian and European government and defense organizations.

A Zero-Day Spotlight on CVE-2024-44308, CVE-2024-44309, and CVE-2024-49039:

A look into zero-days discovered by GTIG researchers

Spotlight #1: Stealing Cookies with Webkit

On Nov. 12, 2024, GTIG detected a potentially malicious piece of JavaScript code injected on https://online.da.mfa.gov[.]ua/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4. The JavaScript was loaded directly from the main page of the website of the Diplomatic Academy of Ukraine, online.da.mfa.gov.ua. Upon further analysis, we discovered that the JavaScript code was a WebKit exploit chain specifically targeting MacOS users running on Intel hardware.

The exploit consisted of a WebKit remote code execution (RCE) vulnerability (CVE-2024-44308), leveraging a logical Just-In-Time (JIT) error, succeeded by a data isolation bypass (CVE-2024-44309). The RCE vulnerability employed simple and old JavaScriptCore exploitation techniques that are publicly documented, namely:

- Setting up addrof/fakeobj primitives using the vulnerability
- Leaking StructureID
- Building a fake TypedArray to gain arbitrary read/write
- JIT compiling a function to get a RWX memory mapping where a shellcode can be written and executed

The shellcode traversed a set of pointers and vtables to find and call WebCookieJar::cookieRequestHeaderFieldValue with an empty firstPartyForCookies parameter, allowing the threat actor to access cookies of any arbitrary website passed as the third parameter to cookieRequestHeaderFieldValue.

The end goal of the exploit is to collect users' cookies in order to access login.microsoftonline.com. The cookie values were directly appended in a GET request sent to https://online.da.mfa.gov.ua/gotcookie?.

This is not the first time we have seen threat actors stay within the browser to collect users' credentials. In March 2021, a targeted campaign used a zero-day against WebKit on iOS to turn off Same-Origin-Policy protections in order to collect authentication cookies from several popular websites. In August 2024, a watering hole on various Mongolian websites used Chrome and Safari n-day exploits to exfiltrate users' credentials.

While it is unclear why this abbreviated approach was taken as opposed to deploying full-chain exploits, we identified several possibilities, including:

- The threat actor was not able to get all the pieces to have a full chain exploit. In this case, the exploit likely targeted only the MacIntel platform because they did not have a Pointer Authentication Code (PAC) bypass to target users using Apple Silicon devices. A PAC bypass is required to make arbitrary calls for their data isolation bypass.
- The price for a full chain exploit was too expensive, especially when the chain is meant to be used at a relatively large scale. This especially includes watering hole attacks, where the chances of being detected are high and subsequently might quickly burn the zero-day vulnerability and exploit.
- Stealing credentials is sufficient for their operations and the information they want to collect.

This trend is also observed beyond the browser environment, wherein third-party mobile applications (e.g., messaging applications) are targeted, and threat actors are stealing the information only accessible within the targeted application.

Spotlight #2: CIGAR Local Privilege Escalations

CIGAR's Browser Exploit Chain

In early October 2024, GTIG independently discovered a fully weaponized exploit chain for Firefox and Tor browsers employed by CIGAR. CIGAR is a dual financial- and espionage-motivated threat group assessed to be running both types of campaigns in parallel, often simultaneously. In 2023, we observed CIGAR utilizing an exploit chain in Microsoft Office (CVE-2023-36884) as part of an espionage campaign targeting attendees of the Ukrainian World Congress and NATO Summit; however, in an October 2024 campaign, the usage of the Firefox exploit appears to be more in line with the group's financial motives.

Our analysis, which broadly matched ESET's findings, indicated that the browser RCE used is a use-after-free vulnerability in the Animation timeline. The vulnerability, known as CVE-2024-9680, was an n-day at the time of discovery by GTIG.

Upon further analysis, we identified that the embedded sandbox escape, which was also used as a local privilege escalation to NT/SYSTEM, was exploiting a newfound vulnerability. We reported this vulnerability to Mozilla and Microsoft, and it was later assigned CVE-2024-49039.

Double-Down on Privilege Escalation: from Low Integrity to SYSTEM

Firefox uses security sandboxing to introduce an additional security boundary and mitigate the effects of malicious code achieving code execution in content processes. Therefore, to achieve code execution on the host, an additional sandbox escape is required.

The in-the-wild CVE-2024-49039 exploit, which contained the PDB string **C:\etalon\PocLowIL\@Output\PocLowIL.pdb**, could achieve both a sandbox escape and privilege escalation. The exploit abused two distinct issues to escalate privileges from Low Integrity Level (IL) to SYSTEM: the first allowed it to access the WPTaskScheduler RPC Interface (UUID: **{33d84484-3626-47ee-8c6f-e7e98b113be1}**), normally not accessible from a sandbox Firefox content process via the "less-secure endpoint" **ubpmtaskhostchannel** created in ubpm.dll; the second stems from insufficient Access Control List (ACL) checks in WPTaskScheduler.dll RPC server, which allowed an unprivileged user to create and execute scheduled tasks as SYSTEM.

As detailed in "How to secure a Windows RPC Server, and how not to.," there are three ways to secure an RPC server, and all three were utilized in WPTaskScheduler:

1. **Securing the endpoint:** In **WPTaskScheduler::TsiRegisterRPCInterface**, the third argument to **RpcServerUseProtseq** is a non-NULL security descriptor (SD).
   - This SD should prevent the Firefox "Content" process from accessing the WPTaskScheduler RPC endpoint. However, a lesser known "feature" of RPC is that RPC endpoints are multiplexed, meaning that if there is a less secure endpoint in the same process, it is possible to access an interface indirectly from another endpoint (with a more permissive ACL). This is what the exploit does: instead of accessing RPC using the ALPC port that the **WPTaskScheduler**.dll sets up, it resolves the interface indirectly via upbmtaskhostchannel. ubpm.dll uses a NULL security descriptor when initializing the interface, instead relying on the **UbpmpTaskHostChannelInterfaceSecurityCb** callback for ACL checks:

```
__int64 UbpmEnableTaskHostChannelRpcInterface()
{
  HMODULE ModuleHandleW; // rax
  DWORD LastError; // eax
  DWORD v2; // ebx
  _QWORD *v3; // rcx
  __int64 v4; // rdx

  ModuleHandleW = GetModuleHandleW(L"rpcrt4.dll");
  if ( ModuleHandleW )
  {
    s_pfnI_RpcOpenClientProcess = (int (*)(void *, unsigned int, void **))GetProcAddress(
                                                                            ModuleHandleW,
                                                                            "I_RpcOpenClientProcess");
    if ( s_pfnI_RpcOpenClientProcess )
    {
      LastError = RpcServerUseProtseqEpW((RPC_WSTR)L"ncalrpc", 0xAu, (RPC_WSTR)L"ubpmtaskhostchannel", 0LL)
      v2 = LastError;
      if ( !LastError || LastError == 1740 )
      {
        LastError = RpcServerRegisterIfEx(
                      &RPC_INTERFACE,
                      0LL,
                      0LL,
                      0x21u,
                      0x4D2u,
                      (RPC_IF_CALLBACK_FN *)UbpmpTaskHostChannelInterfaceSecurityCb);
```

Figure 5: NULL security descriptor used when creating "ubpmtaskhostchannel" RPC endpoint in ubpm.dll::UbpmEnableTaskHostChannelRpcInterface, exposing a less secure endpoint for WPTaskScheduler interface

2. **Securing the interface:** In the same **WPTaskScheduler::TsiRegisterRPCInterface** function, an overly permissive security descriptor was used as an argument to **RpcServerRegisterIf3**. As we can see on the listing below, the CVE-2024-49039 patch addressed this by introducing a more locked-down SD.

3. **Ad-hoc Security:** Implemented in **WPTaskScheduler.dll::CallerHasAccess** and called prior to enabling or executing any scheduled task. The function performs checks on whether the calling user is attempting to execute a task created by them or one they should be able to access but does not perform any additional checks to prevent calls originating from an unprivileged user.

```
RPC_STATUS TsiRegisterRPCInterface(void)
{
  signed int v0; // ebx
  char IsEnabled; // al
  const WCHAR *securityDescriptorStr; // rcx
  RPC_STATUS v3; // eax
  __int64 v4; // rcx
  bool v5; // cc
  RPC_STATUS result; // eax
  RPC_BINDING_VECTOR *BindingVector; // [rsp+50h] [rbp+10h] BYREF
  PSECURITY_DESCRIPTOR securityDescriptor; // [rsp+58h] [rbp+18h] BYREF
  PSECURITY_DESCRIPTOR permissiveSecurityDescriptor; // [rsp+60h] [rbp+20h] BYREF

  permissiveSecurityDescriptor = 0LL;
  securityDescriptor = 0LL;
  BindingVector = 0LL;
  v0 = 0;
  ConvertStringSecurityDescriptorToSecurityDescriptorW(
    L"D:P(A;;GR;;;WD)(A;;GR;;;S-1-15-2-1)",
    1u,
    &permissiveSecurityDescriptor,
    0LL);
  IsEnabled = wil::details::FeatureImpl<__WilFeatureTraits_Feature_4281959737>::__private_IsEnabled(&`wil::
  securityDescriptorStr = L"D:(A;;GRGWGX;;;SY)(A;;GRGWGX;;;LS)(A;;GR;;;NS)(A;;GR;;;IU)S:(ML;;NWNXNR;;;ME)";
  if ( !IsEnabled )
    securityDescriptorStr = L"D:P(A;;GA;;;S-1-15-2-1)(A;;GA;;;WD)";
  ConvertStringSecurityDescriptorToSecurityDescriptorW(securityDescriptorStr, 1u, &securityDescriptor, 0LL);
  v3 = RpcServerUseProtseqW(L"ncalrpc", 0xAu, permissiveSecurityDescriptor);
  v5 = v3 <= 0;
  if ( v3 )
    goto LABEL_9;
  result = RpcServerInqBindings(&BindingVector);
  if ( result )
  {
    if ( result > 0 )
      return result | 0x80070000;
    return result;
  }
  v3 = RpcServerRegisterIf3(&RPC_INTERFACE, 0LL, 0LL, 41LL, 1234, 0, 0LL, securityDescriptor);
```

Figure 6: Patched WPTaskScheduler.dll introduces a more restrictive security descriptor when registering an RPC interface

CVE-2024-49039 addresses the issue by applying a more restrictive ACL to the interface; however, the issue with the less secure endpoint described in "1. Securing the endpoint" remains, and a restricted token process is still able to access the endpoint.

Unidentified Actor Using the Same Exploits

In addition to CIGAR, we discovered another, likely financially motivated, group using the exact same exploits (albeit with a different payload) while CVE-2024-49039 was still a zero-day. This actor utilized a watering hole on a legitimate, compromised cryptocurrency news website redirecting to an attacker-controlled domain hosting the same CVE-2024-9680 and CVE-2024-49039 exploit.

Outlook and Implications

Defending against zero-day exploitation continues to be a race of strategy and prioritization. Not only are zero-day vulnerabilities becoming easier to procure, but attackers finding use in new types of technology may strain less experienced vendors. While organizations have historically been left to prioritize patching processes based on personal or organizational threats and attack surfaces, broader trends can inform a more specific approach alongside lessons learned from major vendors' mitigation efforts.

We expect zero-day vulnerabilities to maintain their allure to threat actors as opportunities for stealth, persistence, and detection evasion.

While we observed trends regarding improved vendor security posture and decreasing numbers around certain historically popular products—particularly mobile and browsers—we anticipate that zero-day exploitation will continue to rise steadily. Given the ubiquity of operating systems and browsers in daily use, big tech vendors are consistently high-interest targets, and we expect this to continue. Phones and browsers will almost certainly remain popular targets, although enterprise software and appliances will likely see a continued rise in zero-day exploitation. Big tech companies have been victims of zero-day exploitation before and will continue to be targeted. This experience, in addition to the resources required to build more secure products and detect vulnerabilities in responsible manners, permits larger companies to approach zero-days as a more manageable problem.

For newly targeted vendors and those with products in the growing prevalence of targeted enterprise products, security practices and procedures should evolve to consider how successful exploitation of these products could bypass typical protection mechanisms.

Preventing successful exploitation will rely heavily on these vendors' abilities to enforce proper and safe coding practices. We continue to see the same types of vulnerabilities exploited over time, indicating patterns in what weaknesses attackers seek out and find most beneficial to exploit. **Continued existence and exploitation of similar issues makes zero-days easier; threat actors know what to look for and where exploitable weaknesses are most pervasive.**

Vendors should account for this shift in threat activity and address gaps in configurations and architectural decisions that could permit exploitation of a single product to cause irreparable damage.

This is especially true for highly valuable tools with administrator access and/or widespread reach across systems and networks. Best practices continue to represent a minimum threshold of what security standards an architecture should demonstrate, including zero-trust fundamentals such as least-privilege access and network segmentation. Continuous monitoring should occur where possible in order to restrict and end unauthorized access as swiftly as possible, and vendors will need to account for EDR capabilities for technologies that currently lack them (e.g., many security and networking products). GTIG recommends acute threat surface awareness and respective due diligence in order to defend against today's zero-day threat landscape. **Zero-day exploitation will ultimately be dictated by vendors' decisions and ability to counter threat actors' objectives and pursuits.**


Zero-Days