We're All in this Together

A Year in Review of Zero-Days Exploited In-the-Wild in 2023

2024 March

Google

This report presents a combined look at what Google knows about zero-day exploitation, bringing together analysis from TAG and Mandiant holistically for the first time. The goal of this report is not to detail each individual exploit or exploitation incident, but look for trends, gaps, lessons learned, and successes across the year as a whole. As always, research in this space is dynamic and the numbers may adjust due to the ongoing discovery of past incidents through digital forensic investigations.

We're excited to bring together a broader look at this space with the integration of Mandiant into Google. The report leverages TAG and Mandiant original research, combined with breach investigation findings and reporting from reliable open sources. The numbers presented here reflect our joint understanding, deduplicating how our teams separately may have tracked exploited vulnerabilities in years past. As a result, discerning readers may notice a difference between our numbers here and in prior years' reporting.

This report was authored by Maddie Stone, Jared Semrau, and James Sadowski.

Table of Contents

Executive Summary

Google observed 97 zero-day vulnerabilities exploited in-the-wild in 2023, over 50 percent more than 2022 (62 vulnerabilities), but shy of the record 106 vulnerabilities exploited in 2021. These numbers reflect the combined analysis of Google's Threat Analysis Group (TAG) and Mandiant, brought together holistically for the first time.

We split the vulnerabilities we reviewed into two main categories: end user platforms and products (e.g. mobile devices, operating systems, browsers, and other applications) and enterprise-focused technologies such as security software and appliances.

When we dive into the data, we see progress in defending against zero-days. End user platform vendors, such as Apple, Google, and Microsoft, have made notable investments that are having a clear impact on the types and number of zero-days actors are able to exploit. Vulnerabilities that were commonplace in years past are virtually non-existent today.

On the enterprise side, we see a wider variety of vendors and products targeted, and an increase in enterprise-specific technologies being exploited. Over the years we've learned that the quicker we discover and patch attackers' bugs, the shorter the lifespan of the exploit, and the more it costs attackers to maintain their capabilities. We as an industry must now learn how to take those lessons learned and apply them to the wider ecosystem of vendors that are now finding themselves under attack.

Our key takeaways include:

Vendor investments are making a difference. Vendor investments in exploit mitigations are having a clear impact on the types of bugs attackers are able to exploit in-the-wild. Notable advancements include Google's MiraclePtr preventing exploitation of use-after-free vulnerabilities in Chrome and Apple introducing Lockdown mode for iOS, which successfully prevents exploitation of many exploit chains used in-the-wild.

Attackers shifting focus to third-party components and libraries in 2023. Zero-day vulnerabilities in third party components and libraries were a prime attack surface in 2023, since the exploitation of this type of vulnerability can scale to affect more than one product. We saw this theme repeated across threat actors of all motivations, seeking vulnerabilities in products or components that provided broad access to multiple targets of choice.

Enterprise targeting continues to increase and is more varied in 2023. We observed an increase in adversary exploitation of enterprise-specific technologies in 2023, with a 64 percent increase in the total number of vulnerabilities from the previous year and a general increase in the number of enterprise vendors targeted since at least 2019. This increase was fueled mainly by the exploitation of security software and appliances.

Commercial surveillance vendors (CSVs) lead in browser and mobile device exploitation. CSVs were behind 75% of known zero-day exploits targeting Google products as well as Android ecosystem devices in 2023 (13 of 17 vulnerabilities). Of the 37 zero-day vulnerabilities in browsers and mobile devices exploited in 2023, we attributed over 60% to CSVs that sell spyware capabilities to government customers.

The People's Republic of China (PRC) continues to lead the way for government-backed exploitation. PRC cyber espionage groups exploited 12 zero-day vulnerabilities in 2023, up from seven in 2022, more than we were able to attribute to any other state and continuing a trend we've observed for multiple years.

Exploitation associated with financially motivated actors proportionally decreases. Financially motivated actors accounted for 10 zero-day vulnerabilities exploited in 2023, a lower proportion of the total than what we observed in 2022. Threat group FIN11 exploited three separate zero-day vulnerabilities and at least four ransomware groups separately exploited another four zero-days.

Getting into the Numbers

In 2023, Google's threat intelligence teams tracked 97 unique zero-day vulnerabilities exploited in-the-wild, with the Threat Analysis Group (TAG) and Mandiant accounting for the original discovery of 29 of those vulnerabilities. Following our disclosure policy, Google shares its research to raise awareness and advance security across the ecosystem.

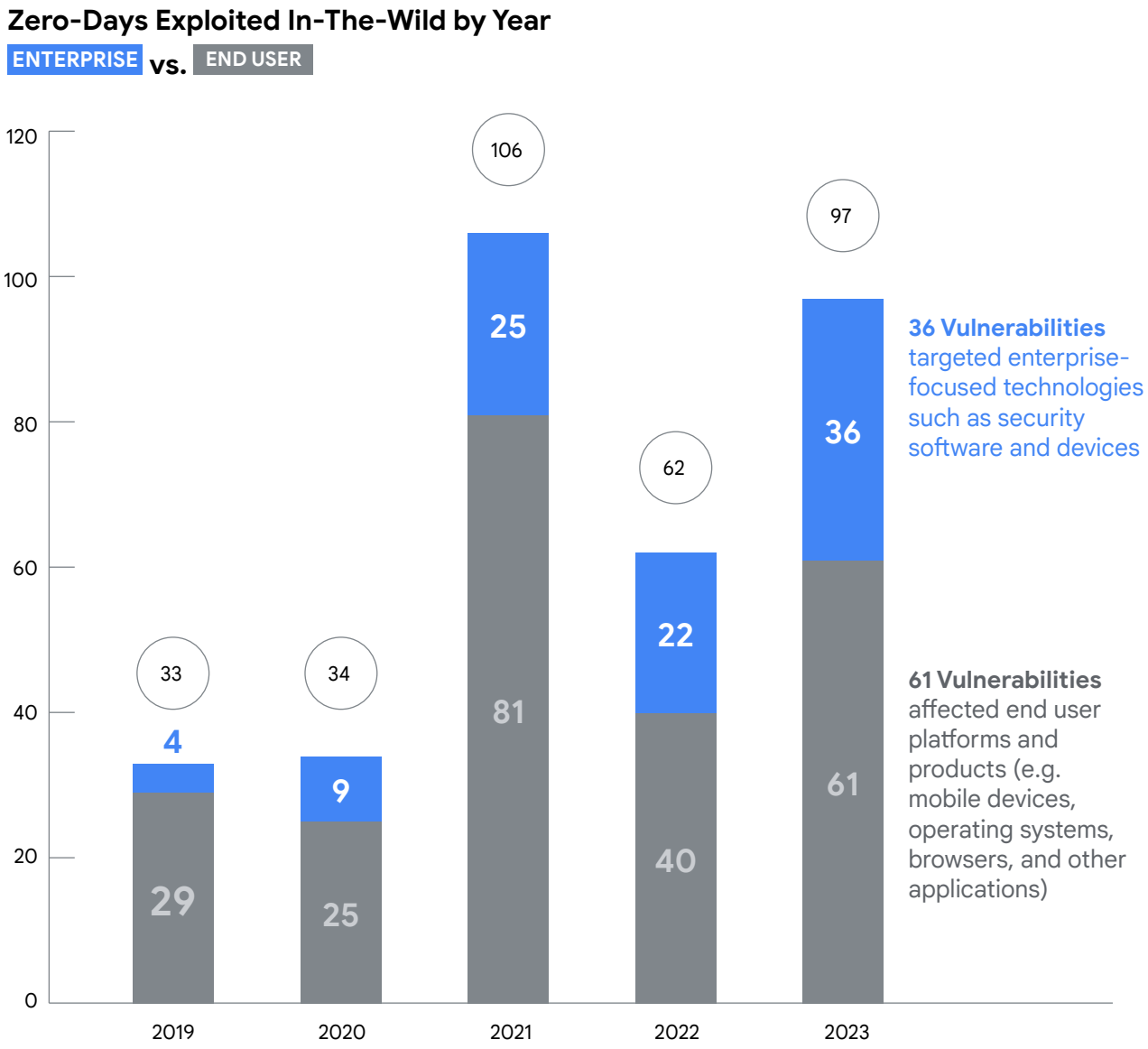


Figure 1. Zero-days exploited in-the-wild by year

Nearly two-thirds of these (61 vulnerabilities) affected end user platforms and products (e.g. mobile devices, operating systems, browsers, and other applications) while the remaining 36 vulnerabilities targeted enterprise-focused technologies such as security software and devices.

End User Platforms and Products

In 2023, we tracked 61 zero-days in-the-wild that specifically targeted end-user platforms and products, which we define as devices and software that individuals use in their day-to-day life, outside of an enterprise environment. This includes mobile devices, operating systems, browsers, and other applications. When we look at the zero-days exploited in-the-wild targeting end-user platforms and products, we see a few common trends:

- Several significant mitigations vendors have developed are effectively preventing exploitation of entire classes of vulnerabilities.
- Vulnerabilities in third party components and libraries are a prime attack surface since they can often affect more than one product.

Primary End-User Platform Zero-Days

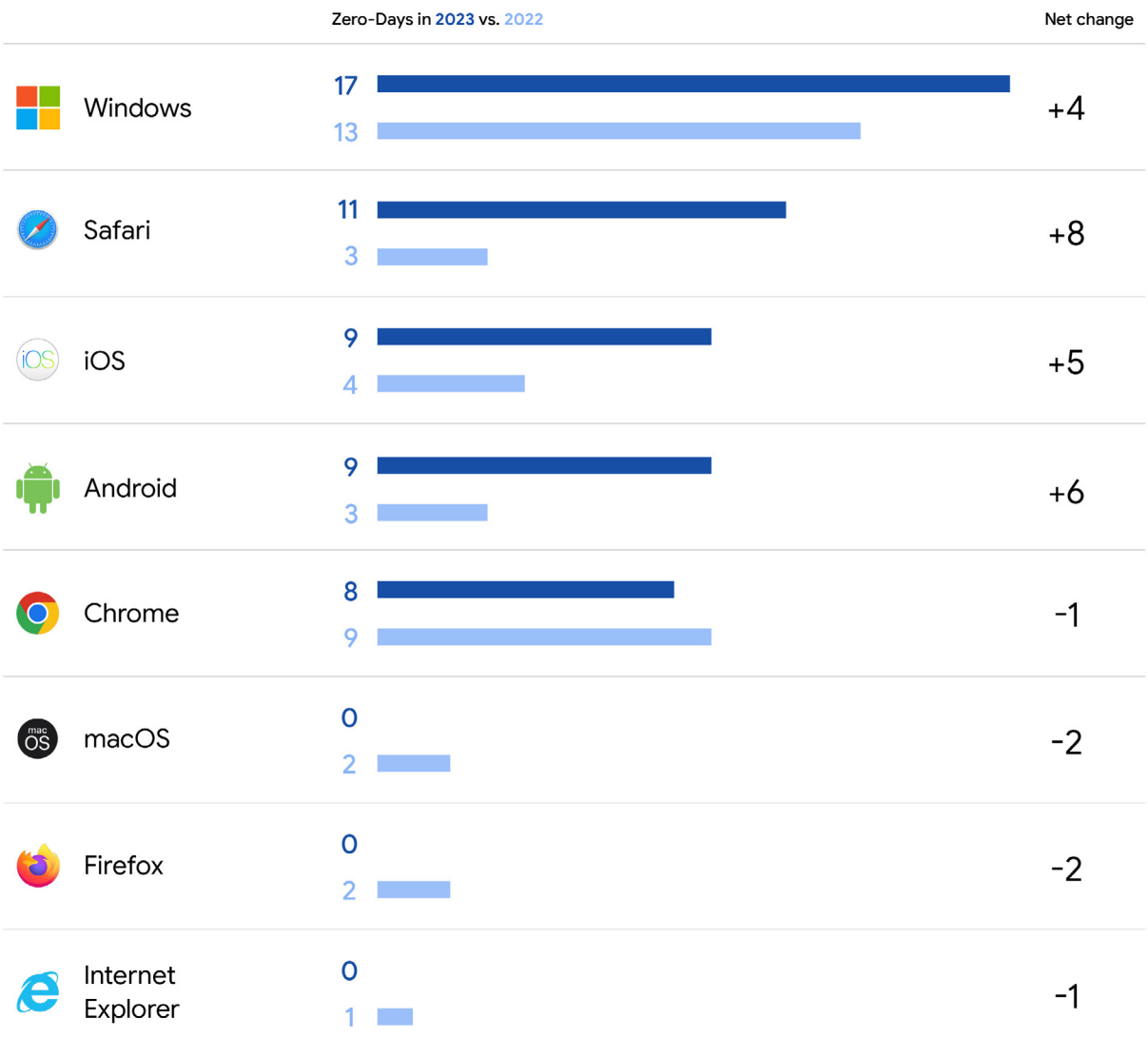


Figure 2. Zero-days in end-user products in 2022 and 2023

Investing in Exploit Mitigation: Platforms are Making Zero-Days Harder

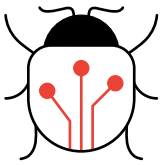
Across browsers and operating systems, investments into exploit mitigations are impacting attackers and the types of vulnerabilities that they're able to use to accomplish their goals.

Out of the eight in-the-wild zero-days targeting Chrome, none of the vulnerabilities were in the Document Object Model (DOM), and not a single one was a use-after-free. Over the past couple of years, Chrome has released multiple exploit mitigations to address the primary vulnerabilities and exploitation techniques seen in years prior. Chrome first announced MiraclePtr in 2022 due to "half of the known exploitable bugs in Chrome [being] use-after-frees." In 2023 there were no use-after-free vulnerabilities exploited in Chrome for the first time since we began seeing Chrome zero days in-the-wild.

Both Chrome and Safari have made exploiting JavaScript Engine vulnerabilities more complex through their V8 heap sandbox and JITCage respectively. Exploits must now include bypasses for these mitigations instead of just exploiting the bug directly.

iOS's Lockdown mode is also making attacker's lives more difficult. If enabled, lockdown mode would have protected users from the majority of the exploitation chains discovered targeting iOS and attackers would not have been able to successfully compromise their targets.

Kudos to Google Chrome and Apple for their investment into exploit mitigations. This demonstrates how these investments are making a real impact on the safety of users and forcing attackers to spend the time to research new attack surfaces and find new bug patterns. We hope to see the continued investment as well as other products and vendors following this lead as well. One of the mitigations we are most hopeful about is the Memory Tagging Extension (MTE) on ARM CPUs. The Pixel 8, released in October 2023, is the first handset to market to include MTE. We're excited about the protection that this can afford high-risk users.



Bugs in Third Party Components on the Rise

In 2023, we saw an increase in 0-days in third-party components and libraries. Vulnerabilities in third-party components tend to be higher value and more useful than vulnerabilities in the product's first party code because they can affect more than just one product. Therefore, an attacker would only need one bug and one exploit to affect two different products instead of developing and maintaining two different ones. While we have seen this a couple of times in past years as well, it occurred more often in 2023, especially across browsers.

In 2023, we saw three browser zero-days exploited that were in third party components and affected more than one browser. We assess with high confidence that the Chrome vulnerability CVE-2023-4863 and the Apple ImageIO vulnerability CVE-2023-41064 are actually the same bug. In addition to Chrome and Safari, it also affected Android and Firefox.

CVE-2023-5217 is the other flaw that affected more than one browser. It is a buffer overflow in libvpx, which is a VP8/VP9 video codec library. This vulnerability affected Chrome, Firefox, iOS, and Android.

There were also two in-the-wild zero-days (CVE-2023-2136 and CVE-2023-6345) in Skia, a 2D graphics library used by Chrome, ChromeOS, Android, and Firefox.

Similar to previous years, the majority of Android in-the-wild zero-days discovered and disclosed in 2023 were in GPU drivers. There were five GPU driver zero-days in 2023: two in the Mali GPU and three in the Qualcomm Adreno GPU driver. As we've discussed before, GPU drivers are a prime attack surface when building exploits for Android devices because the vast majority of Android devices use one of those two GPUs. Attackers can then have coverage for many different devices from different manufacturers, models, etc. with only two different exploits.

Major Platform Spotlights

Year-over-year from 2022 to 2023 we saw most of the big products increase in the number of zero-days detected in-the-wild except for macOS and Chrome. In 2023, there were no in-the-wild zero-days detected that targeted macOS. While some of the iOS vulnerabilities also affected macOS due to their shared kernels and other components, the discovered exploits were only targeting iPhones. For 2023 there was one less Chrome zero-day tracked than in 2022.

In addition to common platforms such as Windows, Android, iOS, Chrome, and Safari, we saw a few other applications targeted with in-the-wild zero-days: WinRAR, Adobe Reader, Microsoft Word, and Microsoft Outlook.

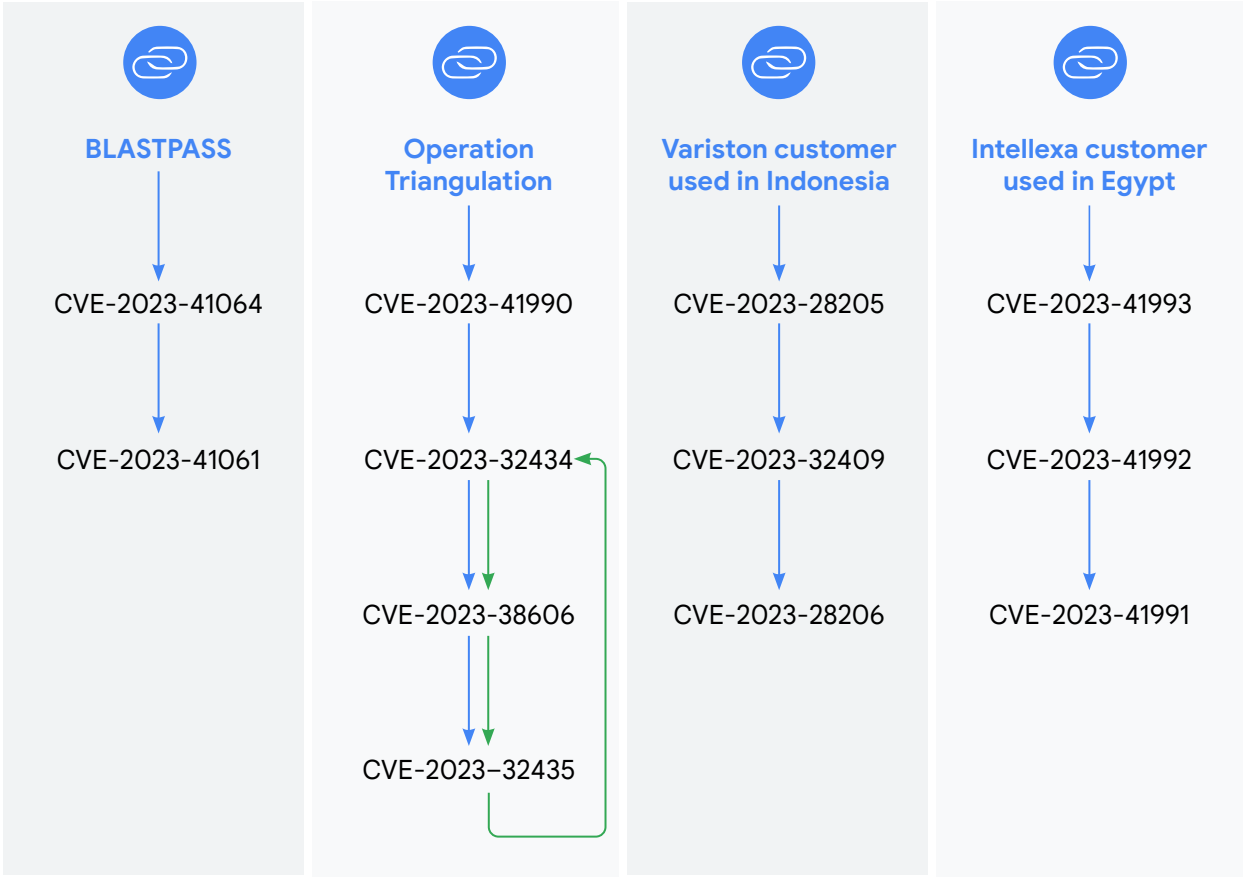


Figure 3. Zero-day exploitation chains targeting iOS detected and disclosed in 2023

Android

There were nine in-the-wild zero-days targeting Android detected and disclosed in 2023, up from three in 2022. In 2022, we assessed the lower number of Android zero-days could have been due to the long life of n-day vulnerabilities functioning as zero-days. While this remains an ongoing issue across the Android ecosystem, we saw fewer in-the-wild exploits this year using n-days that function like zero-days.

Out of the nine Android zero-days for 2023, five were local privilege escalation (LPE) vulnerabilities. Two others were information leaks and the remaining two were in the Android framework and were found to be abused by malware, rather than by commercial surveillance vendors or government-backed attackers. Of the five LPEs, four were in GPU drivers and one was in the Linux kernel.

iOS

There were eight in-the-wild zero-days targeting iOS detected and disclosed in 2023, up from four in 2022. However, only four different exploit chains accounted for these eight vulnerabilities. There were also 11 zero-days targeting Safari that were used to target iPhones.

As additional security boundaries and mitigations are added to products, this increases the number of vulnerabilities required to maintain remote access capabilities such as surreptitiously installing spyware on a device.

Browsers

In 2023 there were eight in-the-wild zero-days targeting Chrome and 11 targeting Safari. While the tracked Safari zero-days were used in chains targeting iPhones, all except for one of the Chrome zero-days were used in chains targeting Android devices. CVE-2023-5217 was discovered by TAG targeting a Windows device, but the rest of the exploits in the chain were not recovered.

Of the 19 total in-the-wild zero-days targeting browsers, nine of the zero-days were in JavaScript engines (JSE) with only one in the Document Object Model (DOM) (in WebKit). For years we've tracked the proportion of remote code execution bugs that are DOM or JSE bugs and historically that's hovered around 60% JSE and 40% DOM. This year DOM exploitation was virtually nonexistent, with exploitation shifting to JSE and third party components.

Windows

There were 17 in-the-wild zero-days in Microsoft Windows: 12 zero-days that crossed security boundaries such as local privilege escalations or remote code executions and five "security-in-depth" bypasses for "SmartScreen" and "Mark of the Web."

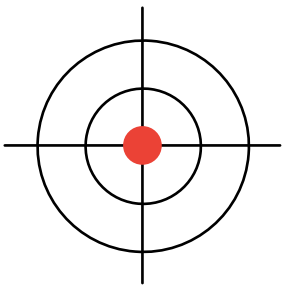
Of the 12 vulnerabilities that crossed security boundaries, nine were local privilege escalation (LPE) vulnerabilities. Following the trends from the last few years, we're seeing a wide variety of components targeted for LPEs, in contrast with 2019 where more than 50% of the in-the-wild zero-days targeting Windows were in Win32k. Today, attackers must research and develop exploits for many more components to maintain their zero-day capabilities, rather than primarily relying on a single component, like Win32k. This has been driven by Microsoft's work over the last few years to lock down Win32k as an attack surface.

Zero-Days Targeting Enterprise Technologies Increase in Number and Variety

In 2023 we observed 36 zero-days in-the-wild targeting enterprise specific technologies. This emphasizes multiple recent trends Mandiant has identified, with increasing diversity in the types of products that are being exploited and a decreased reliance on browser-based and document-based exploits to be successful. In fact, the percentage of zero-days impacting enterprise technologies slightly outpaced overall in-the-wild growth in 2023 and has been rapidly increasing over the last five years. While only 11.8 percent of zero-days in 2019 affected enterprise technologies, this percentage increased to 37.1 percent in 2023, signaling a continued shift in the types of products targeted for malicious exploitation.

This observed increase in enterprise targeting was fueled mainly by exploitation of security software and appliances, including, but not limited to, Barracuda Email Security Gateway, Cisco Adaptive Security Appliance, Ivanti Endpoint Manager Mobile and Sentry, and Trend Micro Apex One. In total, we observed exploitation of nine vulnerabilities affecting security software or devices. Security software is a valuable target for attackers because it often runs on the edge of a network with high permissions and access. By successfully exploiting such technologies, attackers can gain an initial foothold into a targeted organization for follow-on activity.

While the end user space has been dominated by comparatively few major vendors over the years, the targeting of enterprise technologies features higher variance of vendors and products targeted each year. In 2023, Ivanti and North Grid Corporation had the most zero-days for enterprise technologies with three apiece. Prior to 2023, only Ivanti had been exploited for zero-day exploitation previously, once as recently as 2021 (CVE-2021-22893), illustrating a key challenge many vendors face when they find themselves in unfamiliar territory: learning how to respond to sophisticated attacks targeting their products in a timely and effective manner while simultaneously developing an effective patch that addresses the ways threat actors are weaponizing the vulnerability.



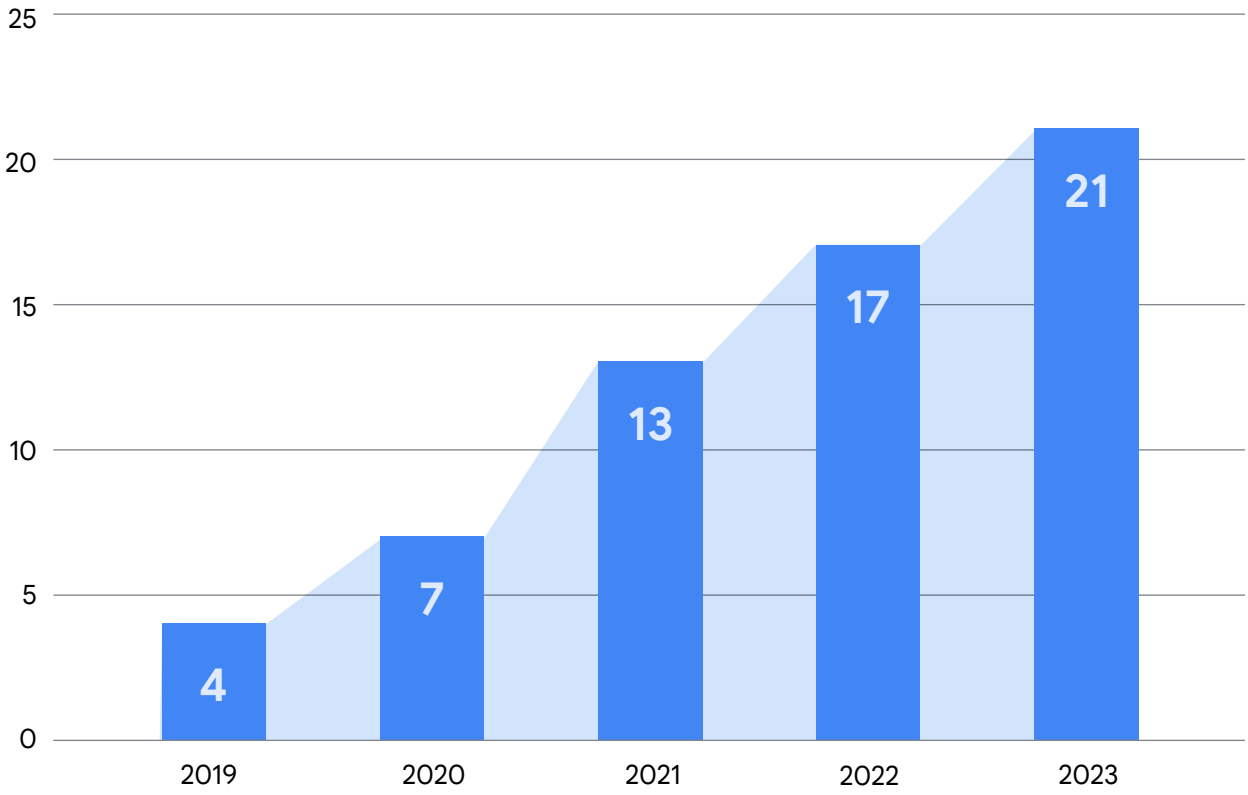


Figure 4. Number of unique enterprise vendors targeted

For enterprise technology vendors, and as an industry as a whole, we must take these lessons learned and apply that knowledge to other vendors who may be inexperienced in these types of responses, or are just being asked to respond for the first time. Microsoft, Apple, and Google are just some examples of software vendors who have more experience in responding to zero-days, but even they are still finding ways to improve how they can triage vulnerabilities, better understand root causes, and develop solutions to address entire classes of vulnerabilities and not just individual flaws.

Old Threat Actors Return, but New Actors Also Join the Cast

Not all zero-day vulnerabilities are equal in the skill needed to exploit them and the types of campaigns in which they're used. Our 2023 analysis spans a commercial surveillance vendor (CSV) industry that develops exploits against end-user products and platforms for use in highly targeted operations by government actors; classic cyber espionage enabled by zero-day exploitation; and financially motivated actors incentivized to develop zero-day exploits that enable efficient and effective monetization of ransomware and extortion attacks.

In 2023, we attributed to commercial surveillance vendors (CSVs) and government espionage actors a combined 48 of 58 zero-days for which we could attribute motivation and only 10 vulnerabilities to financially motivated actors. The proportion (roughly 17%) in 2023 of financially motivated exploitation is slightly lower than our observations from 2022, and both of these years were down from the nearly one-third of vulnerabilities we attributed to financially motivated actors in 2021.

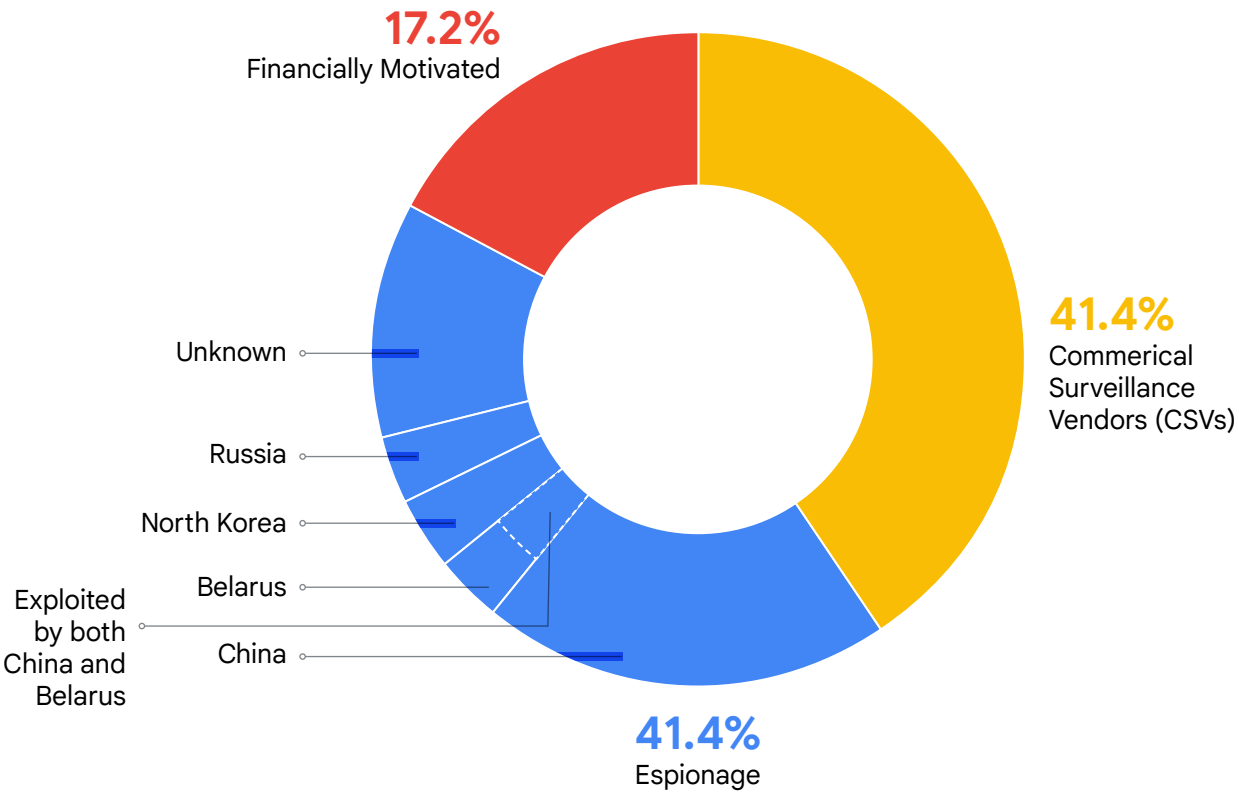


Figure 5. We attributed actor motivation for 58 zero-days in 2023, broken down by commercial surveillance vendors (CSVs), government espionage actors, and financially motivated actors.

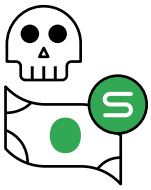
Commercial Surveillance Vendors Focus on End-User Products and Platforms

CSVs were behind 75% of known zero-day exploits targeting Google products and Android ecosystem devices in 2023 (13 of 17 vulnerabilities) as well as 55% targeting iOS and Safari (11 of 20 vulnerabilities). The commercial surveillance industry has emerged to fill a lucrative market niche: selling cutting edge technology to governments around the world that exploit vulnerabilities in consumer devices and applications to surreptitiously install spyware on individuals' devices. By doing so, CSVs are enabling the proliferation of dangerous hacking tools.

All of the vulnerabilities we attributed to CSVs in 2023 targeted mobile devices and browsers, and CSVs accounted for 64% of all mobile and browser vulnerabilities exploited (24 of 37). CSVs operate with deep technical expertise to offer 'pay-to-play' tools that bundle an exploit chain designed to get past the defenses of a selected device, the spyware, and the necessary infrastructure, all to collect the desired data from an individual's device. Government customers who purchase the tools want to collect various types of data on their highest value targets, including passwords, SMS messages, emails, location, phone calls, and even record audio and video. In order to collect this data, CSVs often develop spyware to target mobile devices.

Notably, we could not attribute any Windows zero-days to CSVs. Instead, for the Windows exploitation we could attribute to a threat actor, every instance was from government-backed cyber espionage groups or financially-motivated attackers. We know that Candiru, a CSV, had a chain for Windows because we were able to recover their first stage Chrome exploit, but we were not able to recover the rest of the exploits in the chain.

Ultimately, CSVs, and their government customers using these capabilities, conducted half of attributed zero-day exploitation by government actors in 2023 (24 of 48 vulnerabilities). Private sector firms have been involved in discovering and selling exploits for many years, but we have observed a notable increase in exploitation driven by these actors over the past several years. Additional details on the CSV ecosystem and their role in zero-day exploitation can be found in TAG's February 2023 report Buying Spying: Insights into Commercial Surveillance Vendors.



PRC Groups Again Dominate Government Exploitation, But New Actors Join the Field

We attributed 12 separate zero-day vulnerabilities in 2023 to PRC government-backed actors, with two distinct clusters accounting for the exploitation of five of those vulnerabilities: UNC3886 and UNC4841. Consistent with the two preceding years, we attributed more government-backed exploitation of zero-day vulnerabilities to PRC government-backed attackers than any other state.

Mandiant reported extensively on several widespread exploitation campaigns, including UNC4841's exploitation of two vulnerabilities in Barracuda's Email Security Gateway (CVE-2023-2868 and CVE-2023-7102).

- The actor showed specific interest in information of political or strategic interest to the PRC government, targeting global governments and organizations in high priority industries. Further, we observed specific interest in email domains and users from Ministries of Foreign Affairs of ASEAN member nations as well as individuals within foreign trade offices and academic research organizations in Taiwan and Hong Kong.

UNC3886 exploited three separate zero-day vulnerabilities in campaigns that employed two novel attack paths. The significant period of undetected exploitation of these vulnerabilities demonstrates this actor's objective to remain in target environments and surreptitiously collect information.

- In one path, UNC3886 took advantage of a path traversal vulnerability in Fortinet's FortiOS (CVE-2022-41328) to overwrite legitimate files in a normally restricted system directory before exploiting an authentication bypass vulnerability in VMWare products (CVE-2023-20867) that enabled the execution of privileged commands; we identified this exploitation dating back at least to mid-2022.
- In a different attack path, the group exploited a separate out-of-bounds write vulnerability in VMWare products (CVE-2023-34048) before also exploiting CVE-2023-20867, activity which dated back to at least late 2021.

In a notable development, in 2023, we identified zero-day exploitation by a reportedly Belarusian state sponsored cyber group, identified publicly as "Winter Vivern." This exploitation is the first known instance of reportedly Belarusian-linked espionage groups leveraging zero-day vulnerabilities in their campaigns, suggesting the group is growing in sophistication. The activity primarily targeted government organizations that matched the strategic interests of Belarus and Russia.

Financially Motivated Activity Concentrating Into Fewer Groups

As noted above, we attributed roughly 17% (10 vulnerabilities) of zero-day exploitation to financially motivated actors, a lower proportion than what we observed in 2022. Threat group FIN11 exploited three separate zero-day vulnerabilities, accounting for almost one-third of all financially motivated exploitation we were able to attribute in 2023.

- FIN11 appears to have invested heavily in zero-day exploitation in the last several years. From late 2020 to early 2021, the group also exploited multiple zero-day vulnerabilities in Accellion's legacy File Transfer Appliance (FTA), demonstrating a years-long focus by these actors on identifying and exploiting zero-days.

Additionally, we tracked the exploitation of four additional zero-day vulnerabilities by four ransomware families in 2023. Affiliates of the Nokoyawa ransomware reportedly exploited two separate zero-day vulnerabilities (CVE-2023-28252 and CVE-2023-23376), while affiliates of both Akira and LockBit ransomware reportedly separately exploited the same vulnerability as a zero-day (CVE-2023-20269). We also discovered the exploitation of an unpatched security bypass in Microsoft's SmartScreen security feature (CVE-2023-24880), which financially motivated actors used to deliver the Magniber ransomware without any security warnings.

Given the extensive resources invested into identifying and exploiting zero-day vulnerabilities, financially motivated threat actors highly likely prioritize the use of vulnerabilities that provide efficient access to targeted organizations. FIN11 has focused heavily on file transfer applications which provide efficient and effective access to sensitive victim data without the need for lateral network movement, streamlining the steps for exfiltration and monetization. Subsequently, the large revenues generated from mass extortion or ransomware campaigns likely fuels additional investment by these groups in new vulnerabilities.

Outlook

While it is near impossible to predict the number of zero-days for 2024, it remains clear that the pace of zero-day discovery and exploitation will likely remain elevated when compared to pre-2021 numbers. Regardless of the number, it is clear that the steps we as security researchers and product vendors are taking are having an impact on attackers. However, we must recognize that our successes will likely manifest as actors increasingly targeting wider and more varied products, as the tried and true methods increasingly become less viable.

Zero-day exploitation is no longer just a niche capability accessible to only a handful of actors, and we anticipate that the growth we have seen across the last few years will likely continue, as vendors continue to make other avenues of compromise less accessible and as threat actors focus increasing resources on zero-day exploitation. The wider proliferation of technology has made zero-day exploitation more likely as well: simply put, more technology offers more opportunity for exploitation.

While there is cause to be optimistic, it is incumbent on the industry as a whole to continue learning these lessons and do the things we need in order to be successful: share lessons learned on how to patch smarter and not harder, disclose activities that can have impacts on users and enterprises alike, and be prepared and flexible enough to act quickly to shorten the lifespan and viability of these exploits. A deeper dive on these areas and more can be found in our whitepaper "Escaping the Doom Loop" released last year.

For high risk users, we suggest enabling Lockdown mode if you're an iPhone user or MTE if you use a Pixel 8. For Chrome high-risk users we recommend enabling "HTTPS-First Mode" and disabling the v8 Optimizer. To protect high risk user accounts, we offer the Advanced Protection Program (APP), which is our highest form of account security and has a strong track record protecting users.

We believe it is important for organizations to build defensive strategies that prioritize the types of threats that are most likely to impact their environments or their peers as well as the threats that could cause the most damage. While our focus is on zero-days in this report, it's important that organizations first focus on security foundations to ensure that an attacker can't have success with less sophisticated techniques. Force an attacker to use a zero-day. Organizations should also ask their vendors about their response processes when an in-the-wild zero-day is found targeting their product: the disclosure expectations, patching timelines, root cause analysis, etc.

2023 has shown that software and product vendors ought to prepare themselves for how they will respond when an in-the-wild zero-day is discovered targeting their product. Vendors shouldn't sit back assuming that they're not one of the primary vendors who has been historically targeted. Our recommendations on patching and response from previous years still hold true.