Mass exploitation

The vulnerable edge of enterprise security

June 2024 | Stephen Robinson

WITH secure

Contents

1. Executive Summary

WithSecure searched for trends in Edge Service and Infrastructure vulnerabilities using CISA's Known Exploited Vulnerability Catalogue (KEV), Common Vulnerability Scoring System (CVSS) base scores, and Exploit Prediction Scoring System (EPSS) scores. Based on our analysis we have reached the following conclusions:

- 64% of all Edge Service and Infrastructure CVEs in the KEV exist above the 97.5th percentile of EPSS scores (a metric that scores CVEs based on the likelihood of exploitation). Only 23% of all other CVEs in the KEV are above the 97.5th percentile.
- Edge Service and Infrastructure CVEs added to the KEV in the last two years are on average 11% higher severity than other KEV CVEs.
- The number of edge service and infrastructure CVEs added to the KEV per month in 2024 is 22% higher than in 2023, while the number of other CVEs added to the KEV per month has dropped 56% compared to 2023.
- Edge services are extremely attractive targets to attackers. They are exposed to the Internet and they are intended to provide critical services to remote users, and so they can be abused by remote attackers.
- Similarly, Infrastructure devices are attractive to attackers because they are black boxes which are not easily examined or monitored by network administrators, and they do not have EDR software installed. It is difficult for network administrators to verify they are secure, and they often must take it on trust. Certain types of these devices also provide edge services and so are Internet accessible.
- The capability and expertise needed to exploit zero and one-day vulnerabilities is more attainable for financially motivated cyber criminals than ever.
- Multiple researchers have recently observed that mass exploitation is the new primary observed attack vector for ransomware and nation state espionage attackers. Mass exploitation is enabled by vulnerable or insecure Internet accessible services and infrastructure. It is likely that either:
  - Mass exploitation is becoming the primary attack vector because there are so many vulnerable edge services
  - Or attackers and defenders are now more aware of vulnerable edge services due to the prevalence of mass exploitation

2. Introduction

The cyber threat landscape in 2023 and (so far) 2024 has been dominated by mass exploitation. Previous WithSecure reporting on the professionalization of cybercrime noted the growing importance of mass exploitation as an infection vector, but the volume and severity of this vector have now truly exploded. Several recent reports (summarized below) indicate that mass exploitation may have overtaken botnets as the primary vector for ransomware incidents, and there has been a rapid tempo of security incidents caused by mass exploitation of vulnerable software including, but not limited to: MOVEit, CitrixBleed, Cisco XE, Fortiguard's FortiOS, Ivanti ConnectSecure, Palo Alto's PAN-OS, Juniper's Junos, and ConnectWise ScreenConnect.

There is just one thing that is required for a mass exploitation incident to occur, and that is a vulnerable edge service, meaning a piece of software that is accessible from the Internet. Analysis by BitSight based on Internet scanning found that in 2023, 35% of the 1 million organizations they identified had at least one Internet facing device where a detectable KEV CVE was present. The average time

that those vulnerabilities were present before being remediated was 175 days, meaning that 50% of the detectable KEV CVEs in edge services took longer than that to remediate.

What many exploited edge services have in common is that they are infrastructure devices, such as Firewalls, VPN gateways, or Email gateways, which are commonly locked down black box like devices.

Devices such as these are often intended to make a network more secure, yet time and again vulnerabilities have been discovered in such devices and exploited by attackers, providing a perfect foothold in a target network.

This report will explore the trend of mass exploitation of Edge Services and Infrastructure and will put forward several theories as to why they have been so heavily and successfully targeted by attackers.

2.1 Why the KEV?

This report extracts insights from the Known Exploited Vulnerabilities (KEV) catalogue and the National Vulnerability Database (NVD) that are maintained by the US Government's CISA. The KEV is the best publicly available source of actively exploited vulnerabilities, and so it is being used as a sample set to represent CVEs that are being exploited.

The date the vulnerabilities were added to the KEV database have been used throughout the analysis, as opposed to the date the CVEs were disclosed.

The term 'Other CVEs' is used in this document to refer to CVEs which the KEV describes as having a network attack vector, but which are not Edge Service or Infrastructure CVEs.

3. Industry research on initial access vector trends

Symantec published analysis of ransomware incidents investigated by them in 2023, where exploitation of known vulnerabilities in edge services was identified as the new primary vector for ransomware attacks. The report lists a number of CVEs as likely infection vectors, including:

- CVE-2022-47966 - ZOHO ManageEngine
- Multiple Microsoft Exchange Server vulnerabilities
- Citrix Bleed (CVE-2023-4966) - Citrix NetScaler ADC and NetScaler Gateway
- CVE-2023-20269 - Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) VPN Gateways

Two of these (Cisco ASA/FTD and Citrix NetSTwo of these (Cisco ASA/FTD and Citrix NetScaler) are both infrastructure devices and edge services.

In Verizon Business' 2024 Data Breach Investigations Report, Verizon identified that in 2023 14% of all breaches started with exploitation of a vulnerability, a 180% year on year increase. The report notes that 8% of all breaches investigated by Verizon Business in 2023 related to the MOVEit vulnerability, CVE-2023-34362, which would have contributed to the vulnerability exploitation increase significantly.

In Mandiant's M-Trends 2024 report, which provides statistics on their 2023 incident response engagements, they observe that Russian and Chinese espionage actors, as well as financially motivated attackers are intentionally trying to avoid EDR and other detection technologies through targeting edge services.

Exploitation was the most seen initial infection vector and was seen in 38% of intrusions, a 6% increase. The most common vulnerabilities seen as initial infection vectors were the MOVEit vulnerability CVE-2023-34362, CVE-2022-21587 in Oracle E-Business Suite, and CVE-2023-2868 in Barracuda Email Security Gateways.

The report also lists multiple examples of custom malware deployed by Chinese espionage actors onto edge service infrastructure and observes that there are a number of reasons these devices are attractive. These include the fact that defenders have little to no means of monitoring such devices or detecting malicious activity, and that even post incident investigation of is hampered by the strict control maintained by the manufacturers. The report also notes that due to the lack of monitoring on infrastructure devices, living off the land becomes much easier, as attackers can take advantage of in-built files and functionality to simplify their malware, without significantly increasing their risk of detection.

In Coveware's reporting on ransomware activity in 2024Q1, while in almost 50% of cases the initial access vector in ransomware attacks was unknown, the highest known vector was remote access compromise, followed by software vulnerability exploitation. The report states that notable software vulnerabilities exploited in ransomware attacks included:

- CVE-2023-20269 – Cisco ASA/FTD VPN gateways
- CVE-2023-4966 - NetScaler VPN virtual servers
- CVE-2024-1708-9 - ScreenConnect

4. Edge service exploitation

4.1 What is an Edge Service

An edge service is a piece of software which is installed at the edge of a network and is accessible from both the Internet and the internal network. Typically, it is either providing a service to both networks, or it is providing an external service which relies on the internal network in some way, such as a VPN gateway, a managed file transfer server, or a remote access server.

4.2 Why are attackers targeting Edge Services?

Edge services are being targeted by attackers because they are accessible, and because they make a very good initial access point into a network for an attacker. Edge services need to be reachable from the Internet, and providing a service means that they must accept input from remote users, which can then make them vulnerable to any one of a number of different types of vulnerability.

Edge services also tend to provide an excellent ingress point to a network for attackers. They are often intended to provide access to data stored within the network, or to the network itself, and services such as these often seem to be less heavily protected and security monitored than user devices. Unfortunately, while it is typical for network administrators to limit the permissions and accesses of end users, it is still far too common for server software and services to run with more privileges than is actually necessary, maybe even running as the root or Administrator user on servers which are not segregated from the core network by a DMZ.

These characteristics taken in combination with each other mean that edge services are often Internet accessible, unmonitored, and provide a rapid route to privileged local or network credentials on a server with broad access to the internal network.

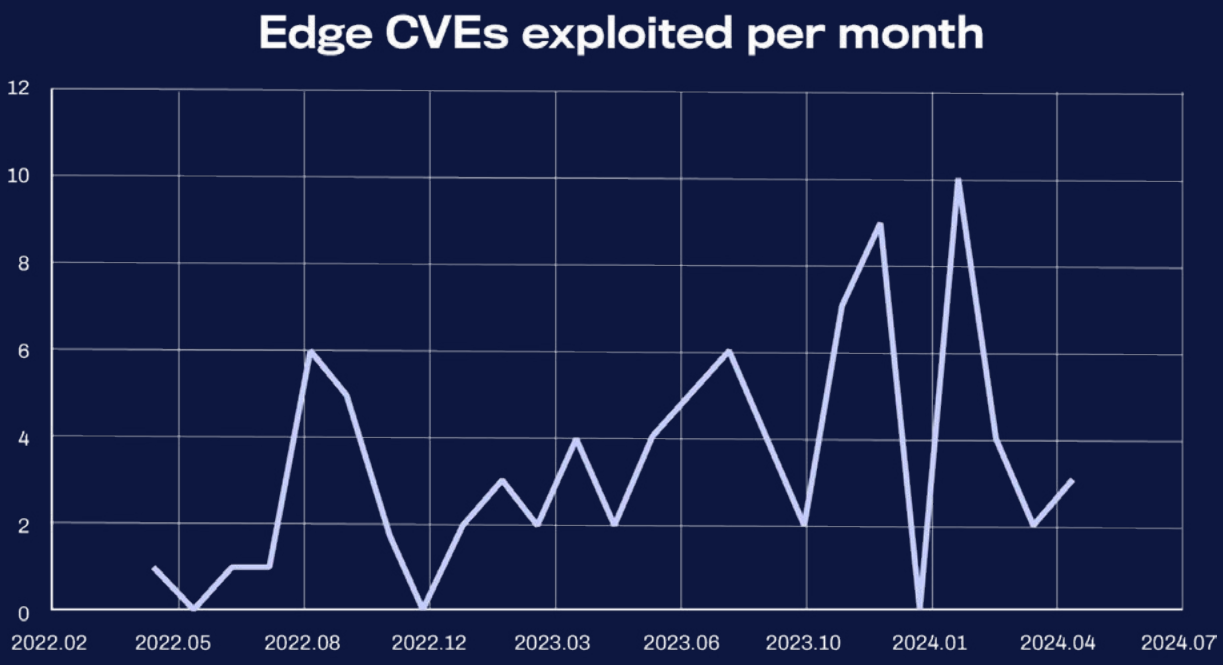
Scanning the Internet to identify vulnerable devices and then exploiting them has been an established method of attack for years, but the rise of Initial Access Brokers (IABs) within the cybercrime marketplace has really driven the industrialization of this activity. Before, an attacker might identify and exploit vulnerable servers, but the number they could monetize was limited by the amount of work they could do. Stealing data or deploying ransomware does after all take time. However, it is now very common for attackers to sell access to compromised devices/networks to other actors, meaning that any device they compromise can be monetized, drastically improving the return on investment of such an activity. Ransomware has also had a more direct effect, as by using it attackers do not need to find valuable data on a network and also a third party willing to buy that data. Instead, they can simply bulk encrypt or steal data then sell it back to the original data owner, who will most likely value it more than any other buyer would. As such, ransomware has incentiv-

ized quantity over quality of intrusions, as almost any compromised network can now be monetized. This in turn suits the indiscriminate, mass exploitation method of gaining initial access. In 2022, small (less than 200 head count) organizations made up 50% of victims posted on ransomware leak sites, but this has increased 5% year on year, so that in 2024 small organizations make up 60% of victims. Payment statistics published by Coveware state that comparing 2023Q4 to 223Q3 ransomware payment rates in dropped to 29%, and the average ransom payment dropped by 33%. Coveware suggest this is due to a decline in the size of victim organizations, which they saw drop by 32% in the same timeframe. Chainalysis' statistics for the whole of 2023 show that total ransom payments doubled compared to 2022 and increased by 10-15% compared to 2021. Together, these statistics could be taken to mean that payment rates and victim sizes are lower, but the total cost is higher, indicating that more, smaller victims are being impacted. It should be noted however that the two research pieces cover different time frames and almost certainly use different data, so they may not be directly comparable in this way.

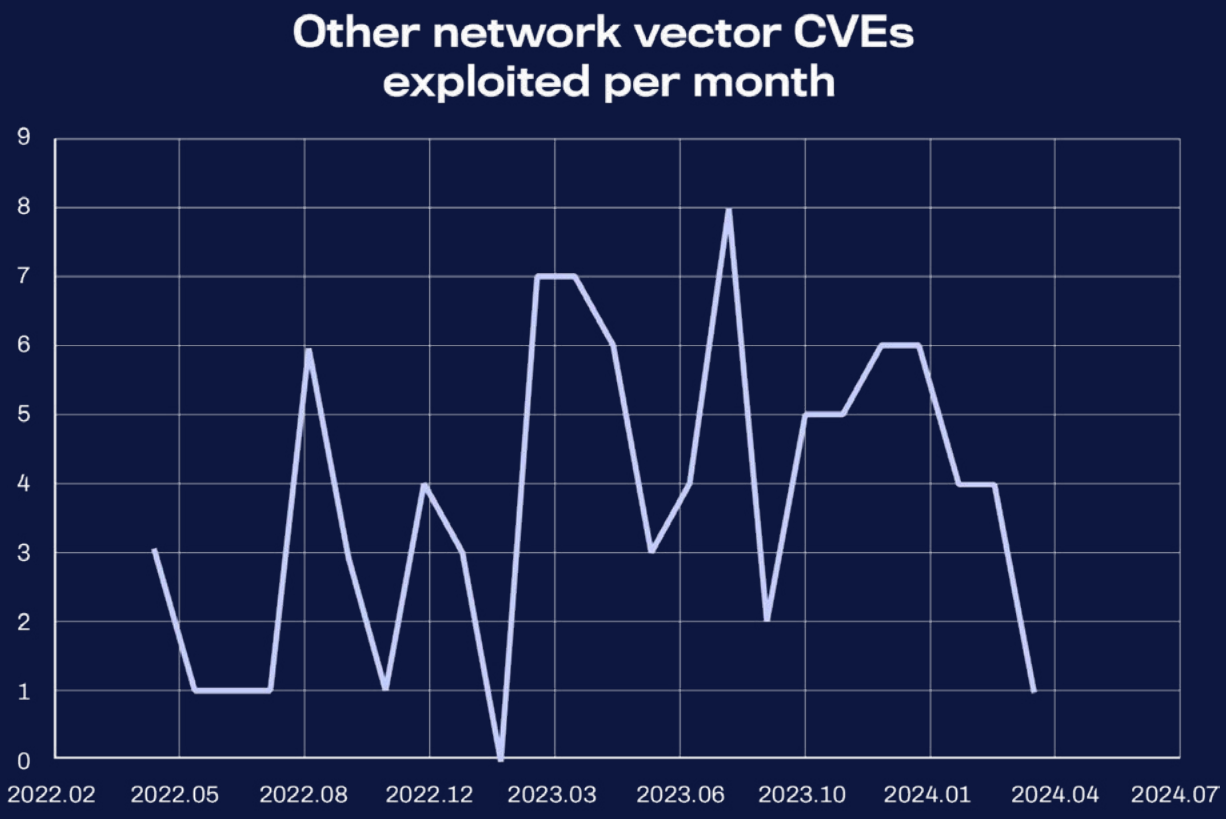
4.3 Edge service KEV vulnerability statistics and trends

4.3.1 Edge CVEs exploited per month

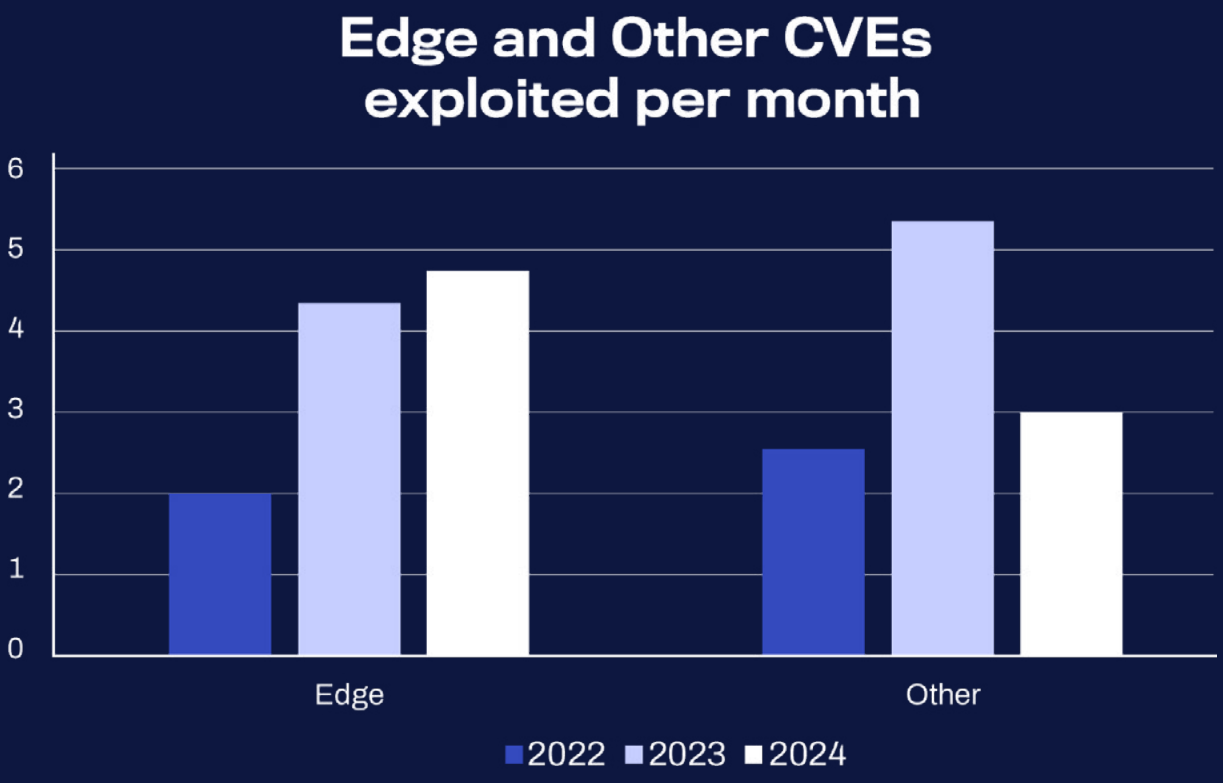
Over the last two years the number of Edge Service CVEs added to CISA's Known Exploited Vulnerabilities catalog (KEV) was relatively low. That number has been trending upwards since the beginning of 2023 however, and it has jumped significantly in the past 6 months, with 8 new edge vulnerabilities added to the KEV in November 2023, and a further 10 in January 2024:



This contrasts with Other (meaning non-Edge, non-Infrastructure, network vector) CVEs, which increased dramatically in 2023, but have since dropped in volume in 2024: This is significant as it means that the increase in Edge and Infrastructure CVEs is not just a quirk of the dataset caused by increased resources or a widened remit for CISA.

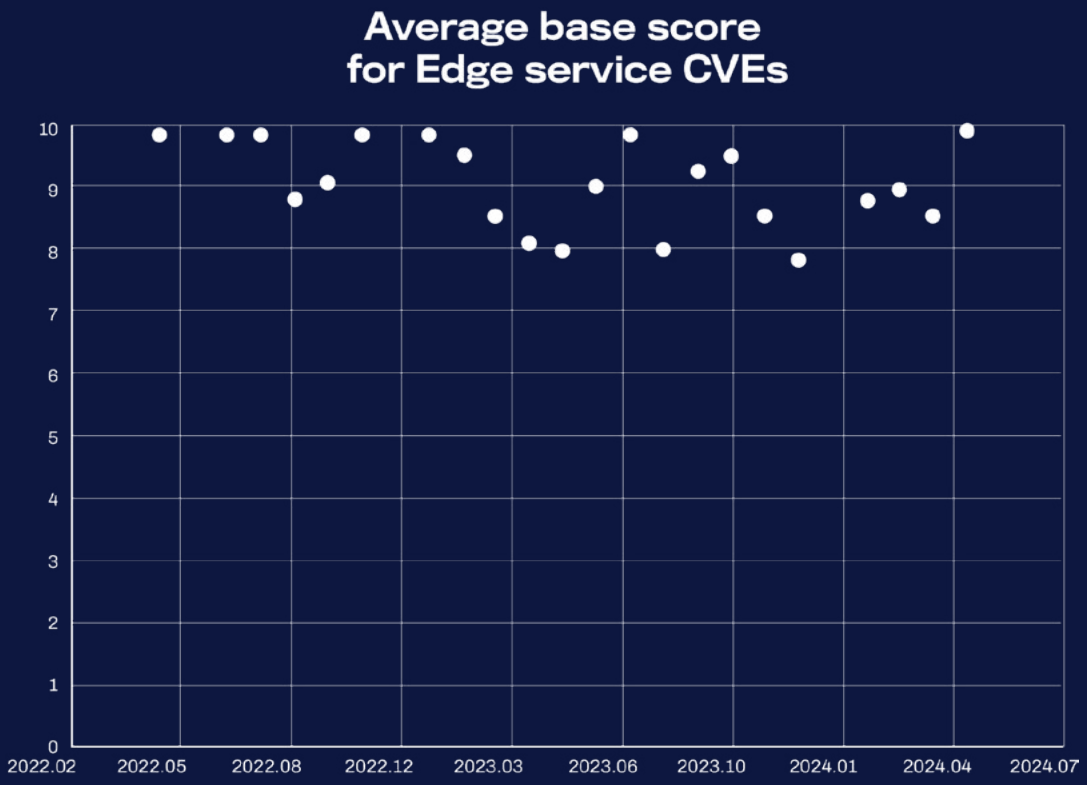


The count of the number of CVEs per month for each year shows a distinct year on year increase for edge services, more than doubling from 2 CVEs per month in 2022 to 4.75 in 2024. This is a very strong trend of continuous increase, especially when compared to Other CVEs. While Other CVEs per month did increase from 2.56 in 2022 to 5.36 in 2023, it has so far dropped to 3 in 2024:

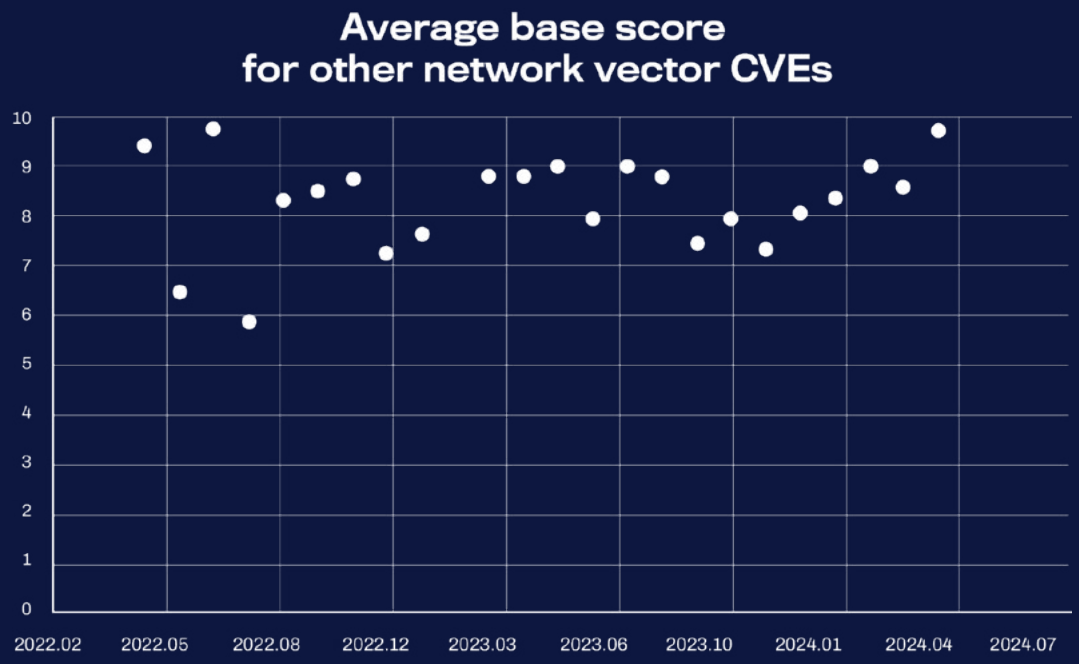


4.3.2 Base score of Edge CVEs

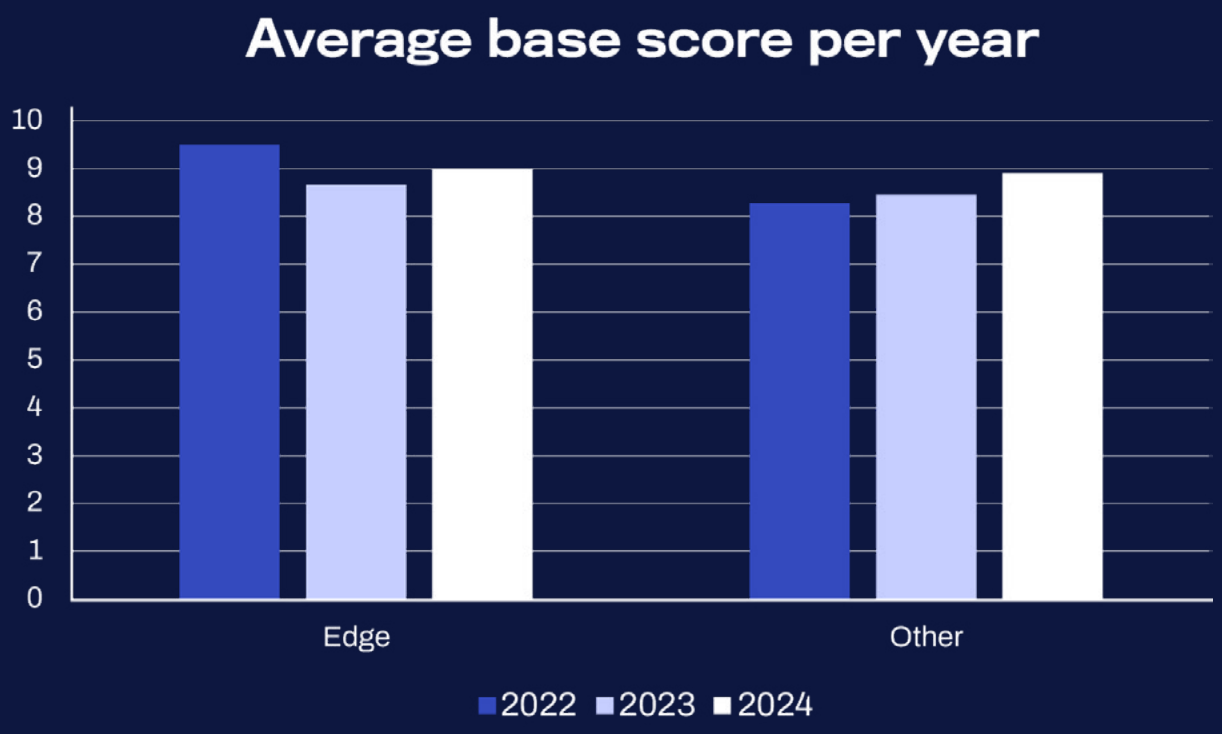
The monthly average base score for Edge CVEs remains consistently high throughout, with very little variance:



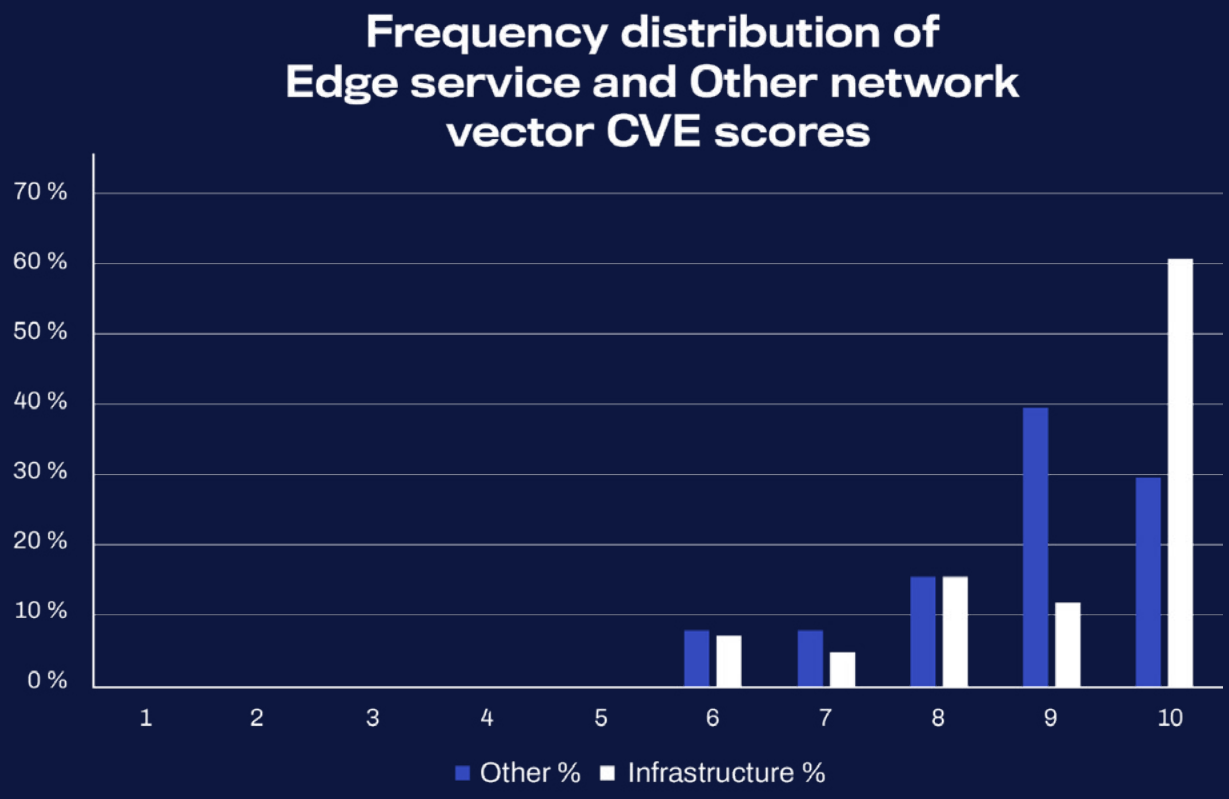
The monthly average base score for Other CVEs each month is generally lower, showing much more variance than Edge service CVEs, though it has trended upwards in 2024:



Looking at the average score per year shows that Edge CVEs scored more severe than Other CVEs each year, although so far in 2024 the difference is only 0.06:



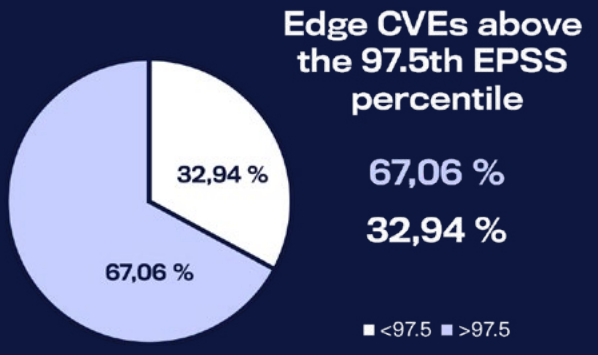
If we look at the frequency distribution, we see an even clearer difference between the two categories, as the median base score for Edge CVEs is 9.8, while the median base score for Other CVEs is 8.8. In fact, 61% of Edge CVEs have a base score in the 9-10 range, while only 30% of Other CVEs are in that range.

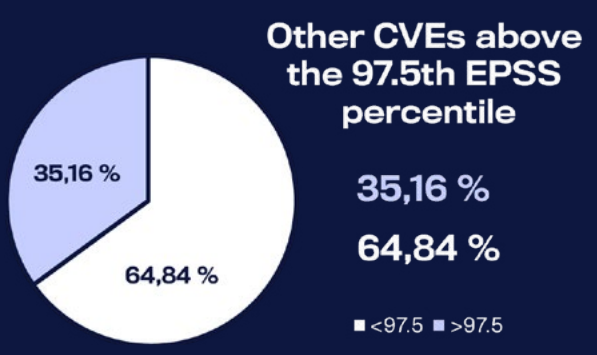


4.3.3 EPSS percentile of Edge CVEs

The EPSS percentile describes how likely a vulnerability is to be exploited in comparison to all other CVEs (not just KEV CVEs). 67.06% of Edge service CVEs were above the 97.5th EPSS percentile:

This is almost the opposite of Other, network vector CVEs, where only 35% were above the 97,5th percentile:

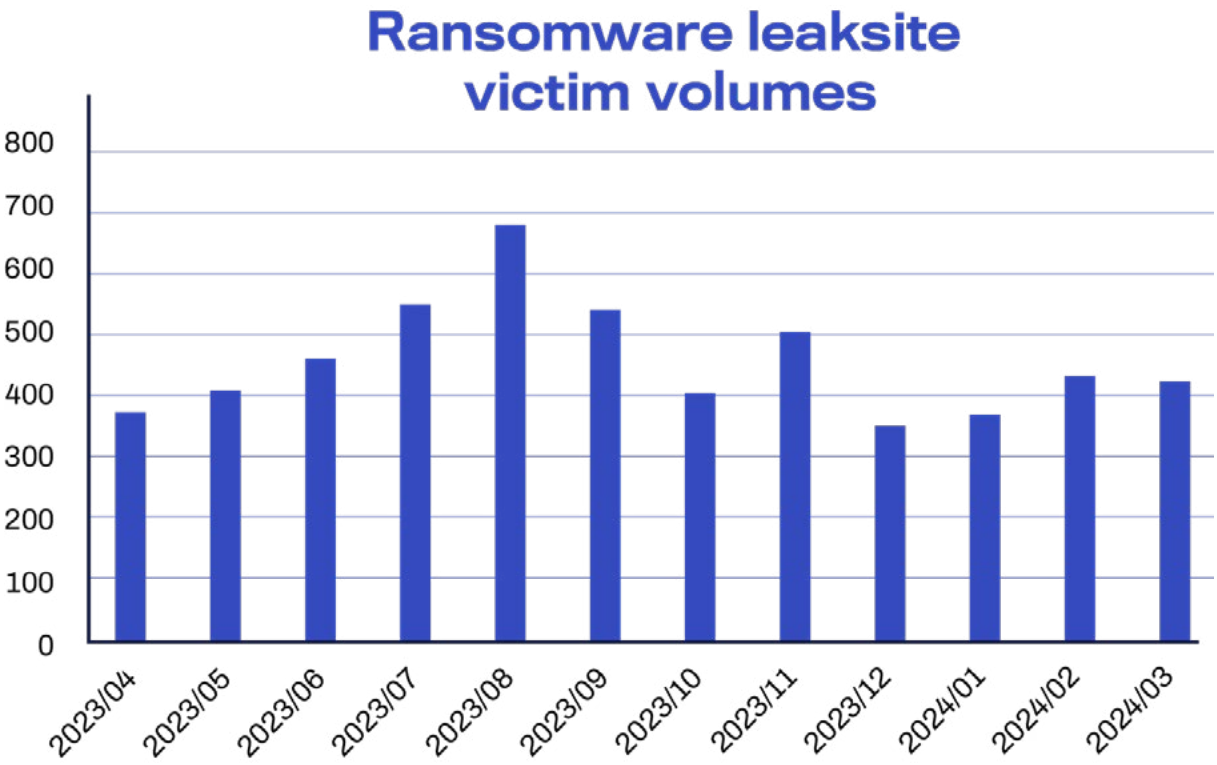




4.4 Major incidents

Multiple major incidents and campaigns have resulted from edge service vulnerabilities and mass exploitation. A small subset of these from 2023 and 2024 are summarized in the sections below. Many of these edge services are web applications which combine multiple complex pieces of software into a single package.

These vulnerabilities have led to tens of thousands of Internet facing services being vulnerable to exploitation, and the nature of edge services has meant that many more organizations and individuals have been exposed to and impacted by such attacks. To take one example, exploitation of MOVEit in mid-2023 impacted almost 3,000 organizations, and as of May 2024 100 million PII records were stolen through MOVEit compromises, although the true number of impacted organizations and individuals may never be known. Looking at the number of victims posted to ransomware leak sites per month illustrates the impact that the MOVEit vulnerability had on the ransomware landscape, showing a clear rise from May 2023, peaking in August:



4.5 What next?

The number and severity of edge service CVEs being exploited by attackers is increasing. Edge services provide an excellent access point and beach head for attackers looking to compromise a network, as has been demonstrated by multiple significant incidents and campaigns in the past year.

Actors often replicate successful attacks and emulate the methods of other successful attackers. This means that once a campaign exploiting a particular vulnerability is publicized, other attackers will likely pile onto the band wagon and begin exploitation. It also means that if a particular vector such as mass exploitation is shown to be repeatedly successful, it is likely that more and more attackers will start to focus on it.

Research published by Symantec, Mandiant, and Coveware in 2024Q1 and Q2 have each stated that mass exploitation is now the primary attack vector for ransomware incidents, and mass exploitation relies upon vulnerable edge services to succeed.

5. Infrastructure exploitation

5.1 What is Infrastructure?

Infrastructure devices, also known as appliances, are devices provided by a supplier as is, with complete supplier defined software and hardware. These devices are commonly sold as a ”black box”, meaning that the inputs and outputs are known, but the actual internal functioning of the device is not. The network administrator may be able to configure the device, but they cannot change the software or hardware beyond supplier set limits. They typically have web and command line interfaces for administration of the functions provided, but the access for the network administrators is restricted. The operating system is almost always a very stripped back version of a *nix operating system. While it may be possible to bypass some restrictions to get an operating system shell, for example via a console port, the majority of the file system partitions will be locked down in such a way as to prevent files being modified.

Along with the practical constraints around these devices, it is almost always the case that if you do change the hardware or modify the software or operating system beyond the supplier’s parameters, the supplier will no longer support the device or honor the warranty. As such, EDR software cannot be installed on them, and the only logs available to an external SIEM are those the supplier has configured.

5.2 Why are attackers targeting Infrastructure?

Infrastructure makes an excellent vector for attackers for a number of reasons. These devices are often installed and then left untouched for years at a time, and then only interacted with via their web-interface or the service they provide. It is not unexpected that they will be running out of date, vulnerable operating systems or software. The devices are almost certainly unmonitored by Endpoint Detection and Response (EDR) software, and as long as they continue to provide the expected services it is very unlikely that anyone will notice if they are compromised by an attacker. Often these devices are active directory integrated, and it may be possible for attackers to extract service or administrator level credentials for Active Directory directly from the appliance device.

These devices typically provide a specific high value service, and these kinds of services can often provide great opportunities to attackers, for example:

Service	Opportunity
VPN	Remote access to the network, interception of user credentials
Email gateway	Email interception, user credentials
Network Attached Storage	File access
Bare metal hypervisor	Access to and control of virtual machines
Network load balancing	Access to critical services and server clusters
Firewall	Bypass of the firewall itself, remote access
Switching or routing	Access to internal network traffic, positioning for ”network local” attacks and poisoning.

Indeed, the value of firewalls and routers to malicious attackers is clearly illustrated by:

- the joint advisory issued in February 2024 by multiple national cybersecurity bodies warning of Russian state sponsored actors targeting and compromising routers for use in cyber operations.
- The CISA and FBI guidance issued in January 2024 urging small office/home office (SOHO) router manufacturers to increase the security of their products in response to targeting and exploitation by Chinese state sponsored actors.

The recent Ivanti ConnectSecure vulnerabilities and associated incidents have provided a good insight into the issues facing infrastructure edge service devices and are explored in the Major Incidents section below.

It is important to remember that while Ivanti has provided an excellent example of the risks that are present and the harms that are possible, it is certainly not the only example of this sort of incident. It is not even the only example of this sort of incident in the first quarter of 2024. Many of the biggest names in network security infrastructure have had multiple, similar incidents, although few seem to have had the level of impact and duration of the 2024 Ivanti cluster-incident.

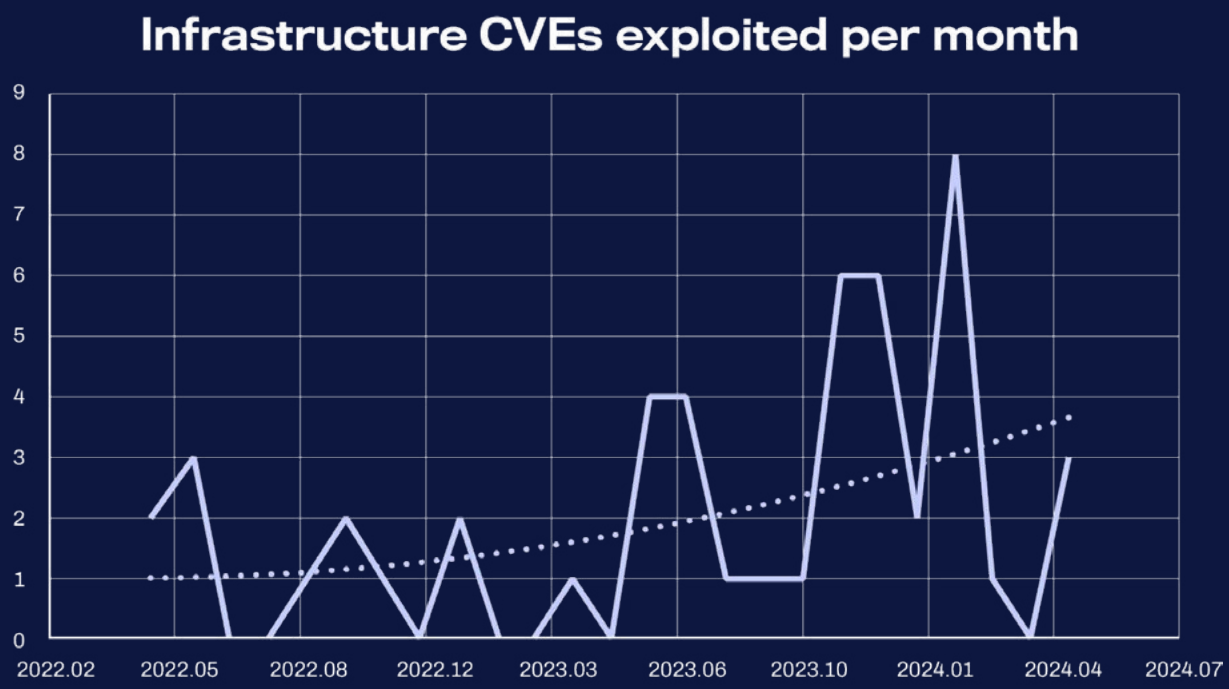
5.3 The EDR problem – EDR isn't installed on appliances/infrastructure

As previously stated, one of the things that makes infrastructure such a good target for attackers is that Endpoint Detection and Response (EDR) agents are not installed on these devices. EDR security software attempts to detect malicious files and behavior on an endpoint, logging, raising alerts, and taking autonomous or administrator approved actions in response. Because EDR is additional, non-standard software for these infrastructure appliances, it cannot be installed without voiding the warranty and support contracts for the devices. As such, these devices don't have EDR installed and become blind spots for security teams, blind spots which we have seen that attackers are all too happy to take advantage of and dwell within.

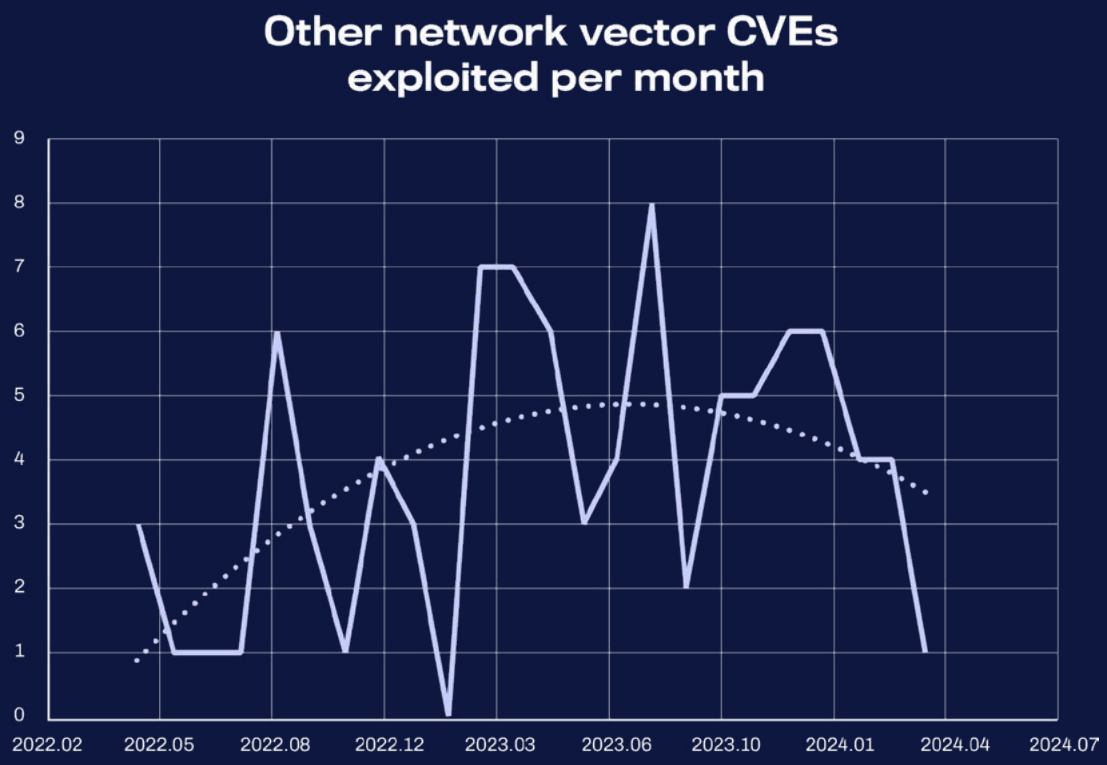
5.4 Infrastructure KEV vulnerability statistics and trends

5.4.1 Infrastructure CVEs exploited per month

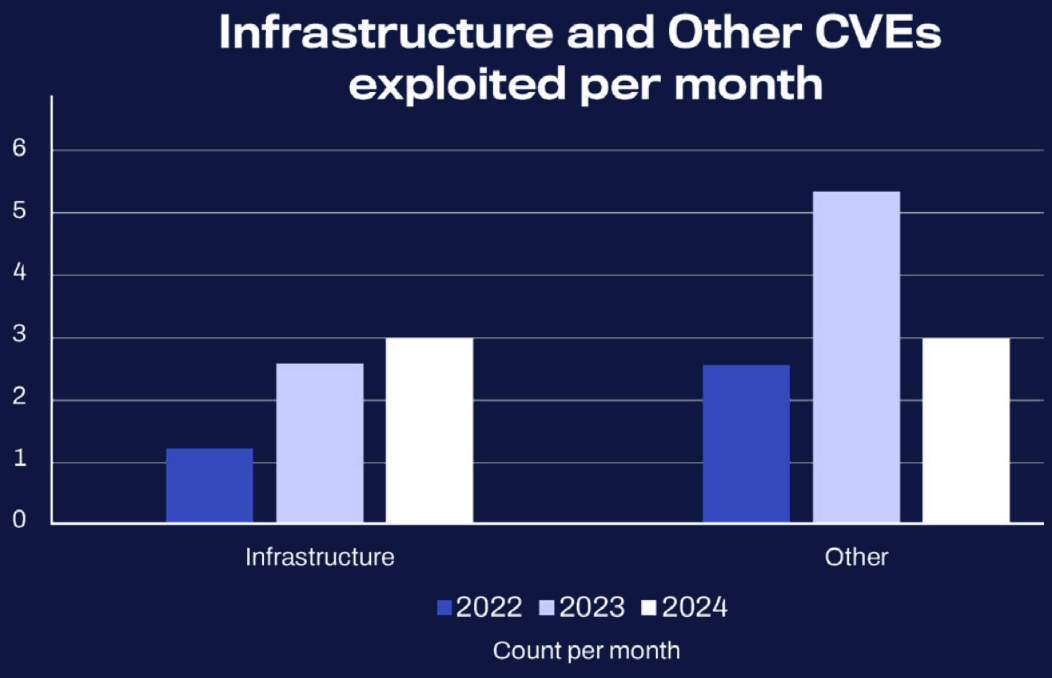
The number of infrastructure CVEs in the KEV has been relatively low over the last two years, but from mid-2023 onwards it began to increase quite drastically, and in January 2024 alone 8 new Infrastructure CVEs were added to the KEV:



This trend was not seen in Other (once again meaning non-Edge, non-Infrastructure, network vector) CVEs:

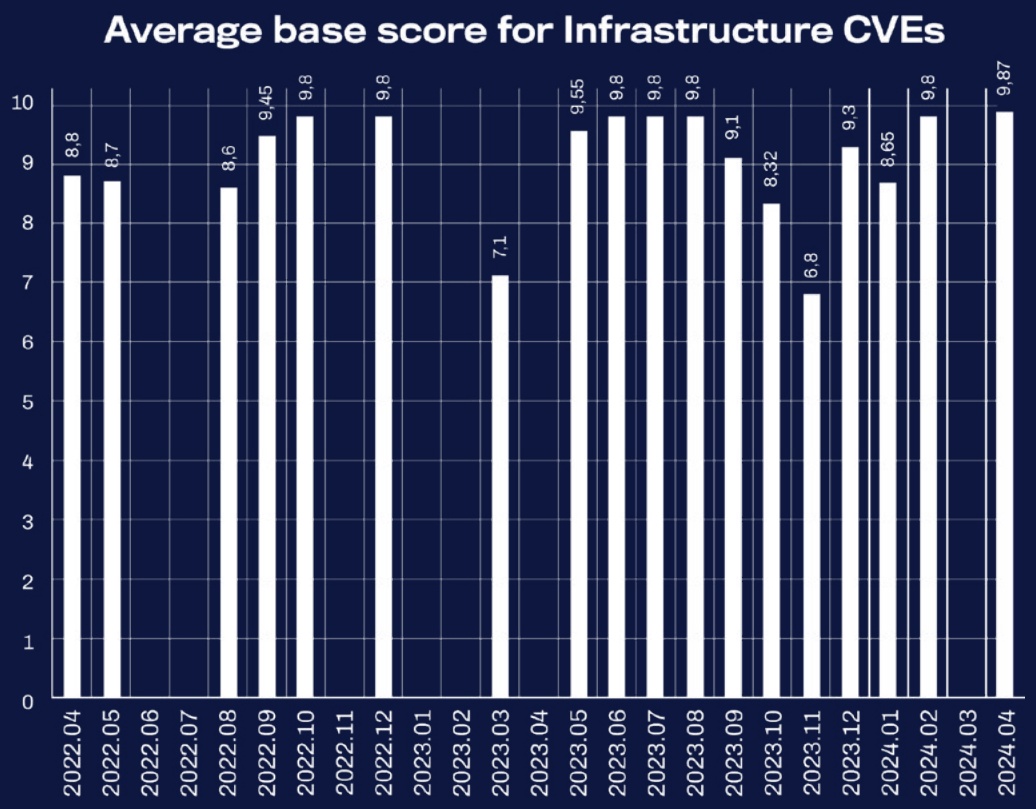


In 2022 the average number of infrastructure KEV CVEs per month was 1.2, rising to 2.6 in 2023, to 3 in 2024. This means that in the first 4 months of 2024 there were almost as many infrastructure CVEs added as in the entirety of 2022:

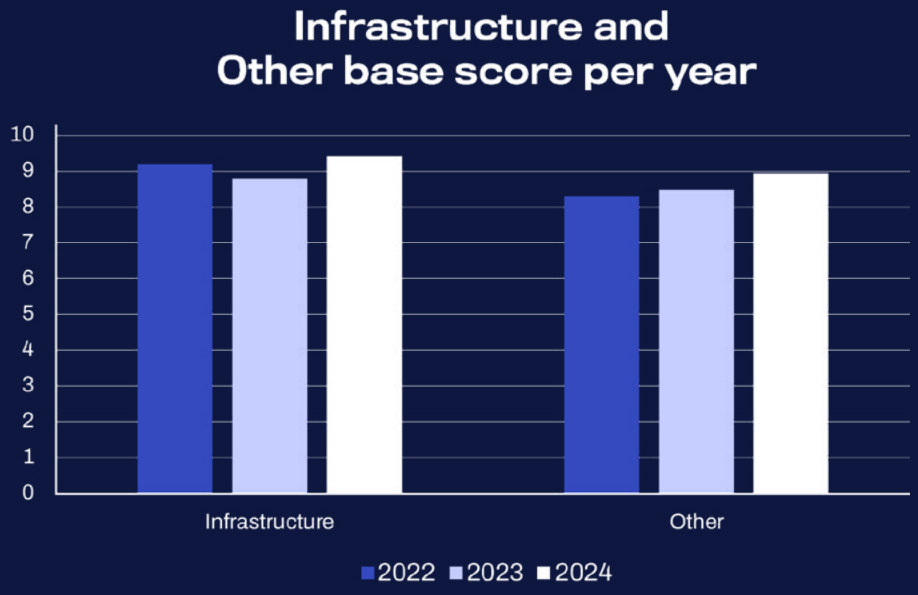


5.4.2 Base score of Infrastructure CVEs

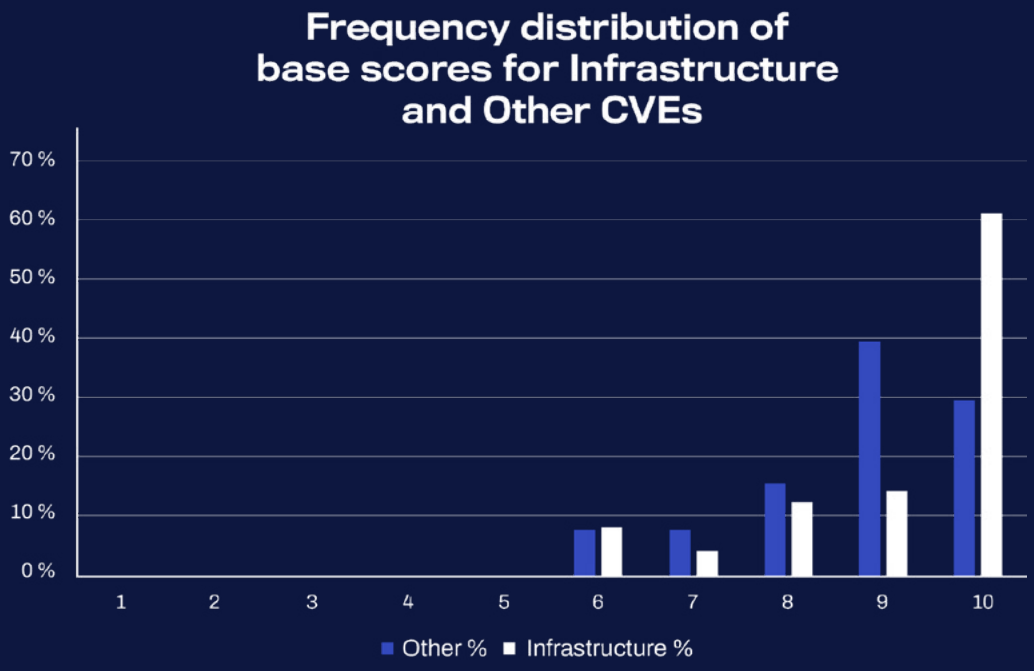
While generally high, there is some variance in the average base score per month for Infrastructure CVEs, with several much lower outliers:



The average severity so far in 2024 is 9.4, compared to the average of Other CVEs which is 8.9:

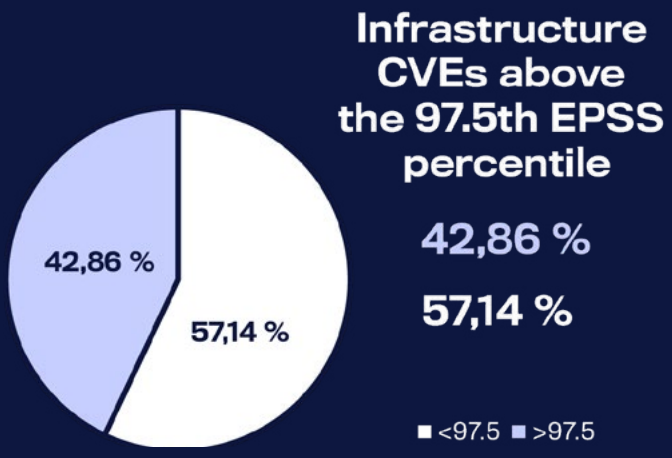


Looking at the frequency distribution of Infrastructure CVE base scores shows a drastic skew towards the top of the scale. The median base score for Infrastructure CVEs is 9.8, and in fact 61% of Infrastructure CVEs lie in the 9-10 range, compared to 31% of Other CVEs, which instead have a median of 8.8:



5.4.3 EPSS percentile of Infrastructure CVEs

42.86% of Infrastructure CVEs were above the 97.5th EPSS percentile, in comparison 35.16% of Other, network vector CVEs were above the 97.5th percentile.



5.5 Major incidents

Multiple major incidents and campaigns have been caused by Infrastructure vulnerabilities.

Often, these vulnerable infrastructure appliances were intended to provide security services and reduce the attack surface, but instead they expanded the attack surface.

One way of estimating the possible impact of these vulnerabilities is the number of Internet exposed devices. It is challenging to get accurate numbers, but rough estimates of the number of Internet exposed Infrastructure devices affected by some of the major infrastructure vulnerabilities of 2024 and 2023 are given below:

Infrastructure Device	Count
Ivanti Connect Secure	26,000
Palo Alto Pan-OS	150,000
Cisco ASA/FDR	320,000
Citrix ADC	60,000
Cisco IOS XE	150,000
FortiGuard FortiOS	250,000
F5 Big IP	16,000
JunOS	11,000
VMWare ESXi	4,000
Barracuda ESG	10,000

In total this gives an estimate of almost 1 million vulnerable infrastructure devices that have been exposed to the Internet. However, by the nature of these devices the impact of a vulnerability is much greater than the possible compromise of a single device, but instead presents the possibility of compromising all of the many devices that interact with and rely upon that infrastructure, which could be a very great number indeed when dealing with enterprise infrastructure. As an example, while a relatively modest 16,000 F5 Big IP devices were observed to be Internet exposed, F5 state that their devices are used by 48 of the top 50 companies in the United States.

Many infrastructure devices run Linux operating systems which have been customized by the supplier. While Linux is seen as a more secure OS, that does of course depend on its configuration, and because Linux is a standard operating system, there are many attackers who are familiar with it and many tools and malware which specifically target it. Many of the devices are difficult for security teams to monitor and intentionally provide a very limited view of the internal workings of the device via their logs. This creates a blind spot which attackers have become aware of and are increasingly seeking to exploit and dwell within. These vulnerabilities have often been found in enterprise infrastructure solutions, where there is typically either a very large install base, or a small install base of very large, high value organizations, both of which are very attractive to attackers. For attackers it is ideal to be able to either compromise a large number of victims at once from which they can then perform victim-agnostic attacks en-masse, or to be able to specifically compromise large enterprises which are likely to each individually be a source of high value data.

5.6 What next?

The volume of exploited Infrastructure vulnerabilities is increasing. While their severity is not increasing, this appears to be because the typical severity of these vulnerabilities is so high, and so close to the top of the CVSS scale that there is simply nowhere further for it to go. It is likely that the main reason why infrastructure CVEs are so high severity is because they are almost always remotely exploitable vulnerabilities with a network attack vector. There will typically be no local access to this type of device, so the only way to exploit them is via the network. Simply due to the way that CVSS scores vulnerabilities, network/remotely exploitable vulnerabilities will be higher scoring.

6. Appendix

6.1 Major Edge Service incidents and campaigns

6.1.1 Progress MOVEit

CVE-2023-35708 was disclosed in June 2023 and was heavily exploited as a zero-day by the Clop ransomware brand against large enterprises and government organizations numbering in the thousands. Proof of concept code became available, and Clop were rapidly followed by other ransomware groups, and most likely nation state actors too.

MOVEit is a managed file transfer service which is used to transfer important data between organizations, as such it is an externally active, Internet accessible service. Important data typically means valuable data, and as such once attackers had compromised these servers they did not need to compromise the network any further to access valuable, ransom-worthy data. They could simply exfiltrate the data available on the server, activity which blended in almost seamlessly with the server's expected, legitimate behavior. Hundreds of major organizations including governments and banks that used the software were compromised, the data of tens of millions of people held by thousands of organizations who did business with the compromised entities was stolen, and it is estimated that Clop received around $100 million in ransom payments from their campaign exploiting this vulnerability.

6.1.2 ConnectWise ScreenConnect

CVE-2024-1708 was announced and patched in ConnectWise ScreenConnect Server in February 2024. This is a remote access/management tool often used by Managed Service Providers (MSPs) to manage the devices of their customers. Legitimate remote management tools are often abused by attackers because they are legitimate tools which provide all the functionality an attacker needs to remotely execute commands and move laterally. Because of the way ScreenConnect is used to provide remote access, often across organizational boundaries, ScreenConnect servers must be accessible to clients. As such this means they are typically edge services accessible from the Internet. The day after the patch was released, proof of concept code became available, and attackers began to exploit the vulnerability. They were then able to use the legitimate remote management functionality of ScreenConnect servers to perform malicious activity on client devices. 5-10,000 ScreenConnect servers were exposed to the Internet at the time the vulnerability was announced, and each server is capable of managing up to 150,000 client devices across multiple organizations.

6.1.3 Zoho ManageEngine ServiceDesk

ManageEngine ServiceDesk is a software which is used to provide service desk and ticketing services for enterprise IT support functions. It is often

remotely accessible so that users who need to raise tickets can do so wherever they are located. Multiple vulnerabilities have been discovered in this software in recent years, and they have been targeted by many different attackers. This was illustrated in WithSecure's Professionalization of Cybercrime report, which detailed an incident where multiple different actors, including Ransomware, IAB, nation state APT, and cryptominer attackers compromised the same ManageEngine ServiceDesk instance..

6.1.4 JetBrains TeamCity

Multiple TeamCity vulnerabilities have been added to the KEV in recent years. TeamCity is a software supply chain tool, and as such it's compromise can provide attackers with the ability to perform supply chain attacks against downstream customers. It also means that TeamCity is key for the day-to-day operation of the organizations using it, and any downtime or data loss from TeamCity, such as through a ransomware attack, is significant. This means that even a localized, non-supply chain attack that takes out a TeamCity instance can be extremely severe. While the number of Internet exposed TeamCity instances is relatively low, somewhere around 2,000 by some estimates the impact that a compromise can cause has made these a priority for attackers and defenders.

6.1.5 Ivanti MobileIron

CVE-2023-35078 in Ivanti's MobileIron Mobile Device Management (MDM) software, was exploited as a zero-day in mid-2023 by attackers targeting the Norwegian government, leading to compromise and data theft from 12 government departments. Because it is an MDM, MobileIron servers need to be accessible to the Internet so that any client mobile device can reach the server. At the time, it was estimates that 5,000 MobileIron servers were accessible to the Internet.

6.1.6 RoundCube Webmail

CVE-2023-5631 is an XSS vulnerability in RoundCube Webmail that was targeted by Russian state sponsored attackers for espionage attacks against European state entities and a think tank. Even though the vulnerability only scored 5.4, it allowed exfiltration of email messages from victims if they simply viewed a specially crafted phishing message. Email web services are ideal edge service compromise targets as they are almost certainly accessible from the Internet, and because they hold huge amounts of valuable organizational information which attackers can download from the email server without touching the rest of the network. Earlier in 2023, this same attacker exploited another XSS in RoundCube Webmail, CVE-2020-35730, in attacks against a very similar set of targets.

6.2 Major Infrastructure incidents and campaigns

6.2.1 Ivanti ConnectSecure

A thorough description of the Ivanti ConnectSecure incident of early 2024 is provided here as it perfectly highlights numerous risks with edge service and infrastructure exploitation.

In January 2024 Ivanti disclosed two zero-day vulnerabilities in their ConnectSecure VPN gateway appliances, which were later found to have been under active exploitation since December 2023. Ivanti Connect Secure (ICS) are edge service, infrastructure devices which run a lightweight Linux operating system which network administrators could not directly access, monitor, or modify. ICS appliances are often configured to authenticate users against Active Directory, and CISA advised that it was trivially easy for attackers to extract Windows Domain Administrator credentials from compromised Ivanti ICS devices, providing full administrator access to Windows networks.

More than 25,000 ICS devices were connected to the Internet, and because these were zero-day CVEs all of them were vulnerable. When the vulnerability was disclosed 10-20 victims had been identified, all of which had been compromised by a single actor. Within days the number of victims compromised by that initial actor had risen to 1,500, and many more distinct campaigns were

observed targeting vulnerable ICS devices. CISA eventually issued advice to US Federal Government agencies that the likelihood of compromise was so high that they should disconnect ICS appliances and assume that their Active Directory domains had been compromised. Because ConnectSecure appliances run the Linux operating system, attackers were able to install standard Linux malware, such as the publicly available Sliver post exploitation framework. Because ICS appliances provide VPN services which users authenticate to, it was also trivially easy for attackers to harvest user credentials for further access and exploitation.

It took 3 weeks from the initial disclosure before patches became available, however Ivanti did release a mitigation tool which was intended to protect devices from compromise. A mitigation tool was required as without a patch there was no action that administrators could take to safely continue using these devices.

Unfortunately, Ivanti then announced that the mitigation tool was flawed, as while it reconfigured devices to prevent exploitation, if any further configuration was pushed to the device via centralized deployment of XML configuration files the mitigation would be removed. Central management and deployment of configuration for enterprise appliances such as these is extremely common.

Ivanti also released an Integrity Checker Tool, which would check if any files on the device had been modified. This was necessary as network administrators are not able to directly access the file system of ICS appliances, so they had no way to verify if a device was compromised except for possibly through very thorough network monitoring of all connections to and from the server. This kind of network traffic collection and monitoring is something that most organizations likely do not have the ability to do.

Attackers and security researchers then proceeded to thoroughly investigate ICS devices, identifying more and more critical vulnerabilities which allowed for remote code execution, as mass exploitation of ICS devices was performed by more and more actors. In one case in February 2024, Orange Cyber Defense observed exploitation of an ICS vulnerability within 5 hours of a Proof of Concept (POC) exploit being published, and within 24 hours they observed more than 600 appliances compromised via that vulnerability.

At the end of February, CISA announced that the ICT that Ivanti was supplying to its customers was not sufficient to detect compromises of ICS devices. For a significant amount of time while Ivanti were working on creating patches for ConnectSecure, the ICT was the only defense available to customers. That, or simply turning off and not using these very expensive enterprise devices that were providing vital VPN remote access to the network for their modern distributed workforces. While Ivanti denied this, they also updated their ICT to address the situation described by CISA.

Security researchers at Eclypsium acquired the ICS operating software/operating system image and bypassed the restrictions around the operating system and file system to examine it. They identified software and OS components that were up to 21 years old, and the Linux kernel for the OS became end of life in February 2016. They found that the majority of the ConnectSecure GUI is written in Perl, which made the 23-year-old Perl version on the appliances a potential problem also. Considering the age of the software used, vulnerabilities in the product are almost to be expected. In the last 21 years software and system design methodologies and paradigms have changed, as have the tools available to developers, and even (we hope) the wider level of security awareness.

ConnectSecure devices, as the name suggests, are intended to provide a secure, Internet facing VPN connection service to protect enterprise networks and remote users. Network administrators who purchased and installed these devices did not know anything about their internal workings, and instead had to simply trust that the supplier was supplying them with a secure solution. As such, there was certainly a strong expectation that the devices would be running modern, secure, software and operating systems. This expectation of security was addressed by the CEO of Ivanti in April 2024 when he released a 6 minute video stating that in response to the security incident the company would begin implementing a 'Secure By Design' ethos for their security products. This was obviously very positive, and also showed real bravery, as it risked criticism from those who might raise concerns as to what the Ivanti design ethos was before this incident.

Victims of compromise via Ivanti ConnectSecure are numerous and varied, but include CISA, the US government Cybersecurity and Infrastructure Security Agency, and MITRE, maintainers of the ATT&CK knowledge base of cybersecurity adversary tactics and techniques.

6.2.2 Citrix ADC/NetScaler – CitrixBleed

CVE-2023-4966, known as Citrix Bleed, probably sits level with the MOVEit vulnerability as the most significant of 2023. CitrixBleed was a zero-day vulnerability in Citrix ADC and NetScaler appliances, which run a lightweight Linux operating system. The vulnerability allowed attackers to steal the session cookies of authenticated users. With these session cookies, attackers could then login to the VPN and access the internal network as if they had legitimate credentials. The theft of session cookies even allowed attackers to bypass multi-factor authentication controls. Estimates of the number of devices running vulnerable versions of Citrix ADC/NetScaler open to the Internet when the vulnerability was announced range from 20,000-60,000. Known victims of CitrixBleed compromises include Boeing, the Industrial and Commercial Bank of China (the 5th largest bank in the world), and US ISP/telecoms giant Comcast Xfinity.

6.2.3 Cisco IOS XE

Cisco network infrastructure devices run several different operating systems, two of which, IOS XE and IOS XR are Linux based. CVE-2023-20198 and CVE-2023-20273 were zero-day vulnerabilities in the web interface of devices running IOS XE which when chained together allowed remote, unauthenticated attackers to create administrator accounts, fully taking over the device. At the time the vulnerability was announced the number of vulnerable devices exposed to the Internet was estimated to be as high as 150,000, and very rapidly 40,000 devices were detected to be compromised by attackers.

6.2.4 Cisco ASA and FDR

Cisco ASA and FDR devices are firewalls that also have VPN gateway functionality. In 2023 ransomware groups breached multiple organizations via their Cisco ASA appliances, and eventually it was discovered that they were exploiting CVE-2023-20269 which allowed them to perform unlimited brute force attacks against the VPN service of the firewalls. Then in early 2024 an older ASA vulnerability, CVE-2020-3259 was exploited in a surge of compromises by ransomware actors including the Akira ransomware brand. According to CISA, Akira received around $40 million dollars in ransoms from their attacks in 2023/4, and repeatedly targeted and compromised Cisco ASA firewalls. Most recently in April 2024, it was disclosed that an espionage campaign that could not be linked to any previously known threat actors had been discovered. This campaign had an unknown initial attack vector and had been exploiting two zero-day vulnerabilities in Cisco ASA/FTD devices (CVE-2024-20353 and CVE-2024-20359) since July 2023. The actor used the compromised firewalls for initial access, reconnaissance, and traffic capture and exfiltration. They were described as having a specific interest in Microsoft Exchange servers and network infrastructure devices from multiple vendors. Over 300,000 Internet exposed Cisco ASA and FDR devices were identified. multiple vendors. Over 300,000 Internet exposed Cisco ASA and FDR devices were identified.

6.2.5 FortiGuard's FortiOS and FortiProxy

FortiGuard make various network infrastructure devices, including VPN gateways. These gateways run a Linux based operating system called FortiOS. In recent years there have been multiple critical zero-day vulnerabilities affecting FortiOS and FortiProxy devices, including CVE-2022-42475, CVE-2022-41328, CVE-2023-27997, and CVE-2024-21762. CVE-2024-21762 allowed unauthenticated attackers to perform remote code execution, and at the time it was disclosed as a zero-day there were an estimated150,000-200,000 FortiGuard devices running a vulnerable version of FortiOS accessible from the Internet.

6.2.6 Palo Alto's PAN-OS

CVE-2024-3400 was a zero-day vulnerability in the GlobalProtect VPN feature of PAN-OS, the Linux based operating system run by Palo Alto firewalls. At the time the vulnerability was disclosed there were more than 150,000 vulnerable PAN-OS devices accessible from the Internet, with multiple actors detected performing remote exploitation.

6.2.7 F5 Big IP

CVE-2023-46747 and CVE-2023-46748 together were exploited as a critical vulnerability chain in F5 Big IP traffic management devices, allowing

remote attackers to execute arbitrary commands. F5 Big IP devices run a Linux based operating system, and 10-20,000 devices were accessible from the Internet. Though it is believed only a small fraction were configured in such a way as to be vulnerable to external attackers, such devices are typically only needed and installed in very large enterprises, and indeed F5 state that 48 of the Fortune 50 list of the largest US companies are using their products.

6.2.8 Juniper's Junos

Multiple High and Critical severity CVEs in Juniper's Junos based devices were disclosed in the last year. Junos is a FreeBSD based operating system. These vulnerabilities include CVE-2024-21591, a remote code execution vulnerability in the J-Web web-based configuration interface, and CVE-2024-21619, and CVE-2024-21620. In January 2024 an estimated 11,000 J-web interfaces of Junos devices were accessible to the Internet.

In April 2024 Juniper issued a patch which addressed 82 separate CVEs in Juniper Cloud Native Routers and Juniper cRPD (essentially a Junos Docker image for cloud deployment). The most notable vulnerability was 9.8 severity CVE-2024-30407, which was due to the use of hard coded private keys in Junos which would allow AiTM attacks to undetectably intercept SSH traffic, resulting in complete compromise of the device. As well as the Junos native vulnerabilities, this patch addressed large numbers of vulnerabilities in external software packages which are included in the OS. Some of the lower severity vulnerabilities were assigned CVEs as far back as 2011, which suggests that the software packages in some versions of Juniper OS may not have been updated since then. There were also six 9.8 severity vulnerabilities in external software packages, which dated back as far as 2019.

6.2.9 VMWare ESXi

IIn 2024, 4 critical vulnerabilities in ESXi were disclosed by VMWare, CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. Several of these vulnerabilities could be chained together to provide full escape from guest VMs to the host hypervisor. While these vulnerabilities are not known to have been used in mass exploitation campaigns by attackers, ESXi is very commonly targeted by ransomware and nation state attackers. By gaining access to a hypervisor attackers can then gain access to the virtual machines it hosts. ESXi is not a Linux based operating system, instead being described by VMWare as a fully custom operating system kernel. However, this does also mean that it is not a standard server and does not run EDR software.

Several ransomware brands have developed ESXi compatible ransomware encryptors, including Akira. Akira gained access to ESXi hosts and encrypted the guest VMs in their attack on the hosting provider Tieto Evry, which impacted multiple government and commercial bodies in Sweden, including the Swedish central bank. Akira did the same again during their 2024 compromise of the Chilean hosting provider IxMetro Powerhost, where they demanded a 2 Bitcoin ransom per customer to be decrypted, presenting a total ransom demand of $140 million. In 2023, the US MGM Casinos organization suffered a ransomware attack where their VMWare ESXi servers were targeted and guest VMs encrypted, resulting in an estimated $100 million loss for the company.

6.2.10 Barracuda Email Security Gateway

CVE-2023-2868 was an unauthenticated remote command execution zero-day vulnerability in Barracuda Email Security Gateway (ESG) appliances which had been under active exploitation by a Chinese state sponsored actor for over 6 months by the time it was discovered and disclosed in late-May 2023. The severity of this vulnerability was such that Barracuda's advice to all customers with ESG appliances was to remove, decommission, and replace them immediately. This implies that the actors were able to compromise these devices so thoroughly, and to so low a level, that it was not possible to evict the attacker even by factory resetting the device and wiping the storage. There were believed to be around 10,000 Barracuda Email Security Gateways accessible from the Internet the week after the vulnerability was disclosed.


WITH
secure