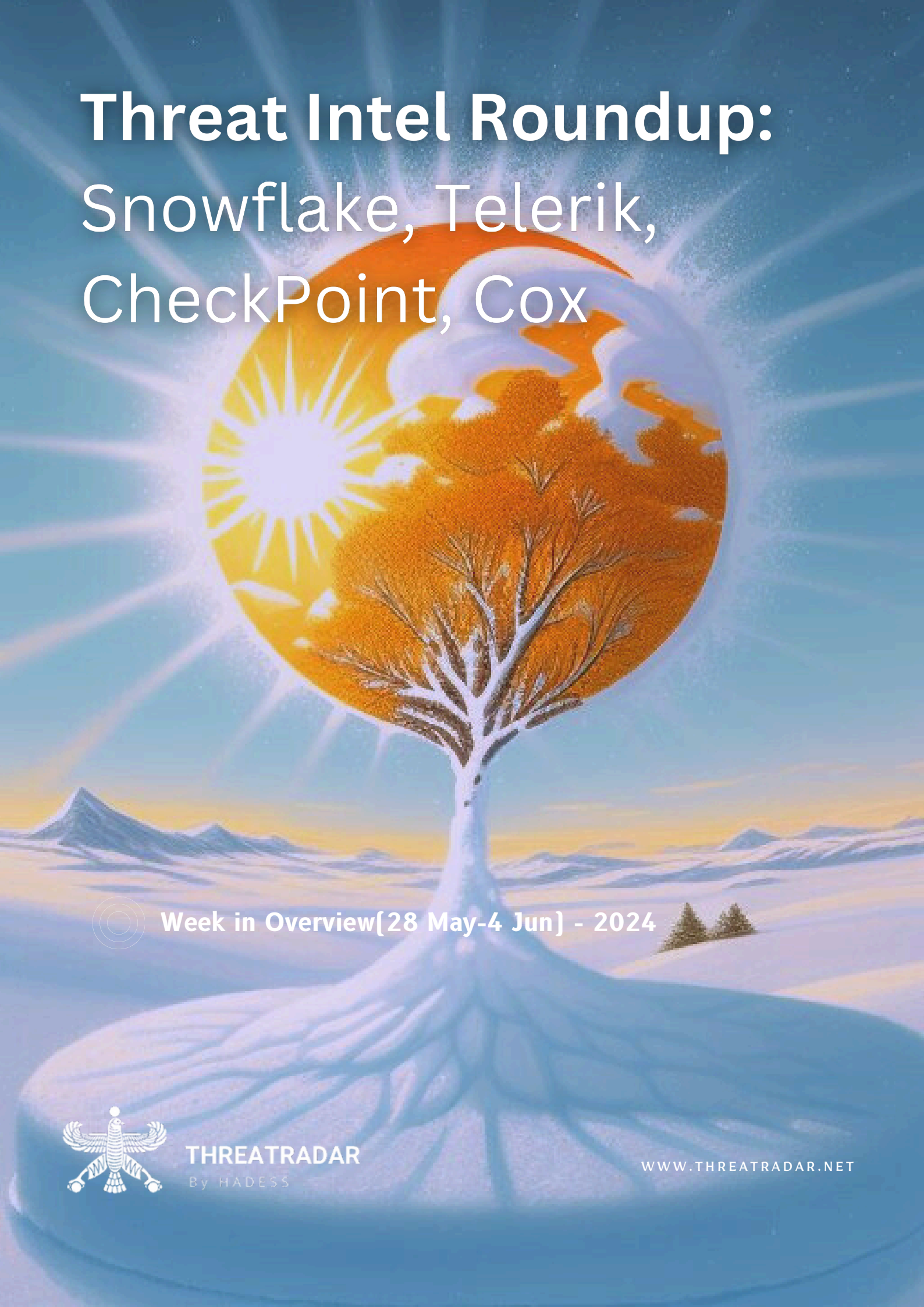
Threat Intel Roundup: Snowflake, Telerik, CheckPoint, Cox



Week in Overview[28 May-4 Jun] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1- CVE-2024-27348 (RCE) - Unauthenticated Users Command Execution via Groovy Injection in Apache HugeGraph-Server
Vulnerability Overview: CVE-2024-27348 is a critical remote code execution (RCE) vulnerability in Apache HugeGraph-Server, identified in versions from 1.0.0 up to versions before 1.3.0. This vulnerability allows unauthenticated users to execute arbitrary commands on the server via Groovy injection. The issue arises due to improper input handling, which permits attackers to inject and execute Groovy scripts.
Impact: The exploitation of this vulnerability can lead to full compromise of the server, enabling attackers to execute system commands, access sensitive data, and potentially further exploit the internal network.
Mitigation: To mitigate this vulnerability, users should upgrade to Apache HugeGraph-Server version 1.3.0 or later. This version contains the necessary patches to prevent Groovy script injection.

2- Snowflake, a leading cloud-based data storage and analytics provider, experienced a security breach in mid-April 2024, disclosed officially on May 23, 2024. The breach involved unauthorized access to its systems, affecting multiple high-profile clients like Santander Bank and Ticketmaster. The breach was attributed to compromised user credentials rather than inherent vulnerabilities in Snowflake's products.
Details:

- The breach was facilitated by a compromised machine used by a Snowflake sales engineer, infected with Lumma Stealer malware.
- The threat actor, known as "Whitewarlock," claimed responsibility and attempted to sell the stolen data back to Snowflake for $2 million.
- Cybersecurity firms identified over 500 demo environment instances in the stealer logs linked to the breach.
- The breach highlights the importance of securing user credentials and monitoring for malware infections.

Impact: Compromised data included sensitive information such as account numbers, credit card details, and employee lists. The breach underscores the need for robust security measures and vigilant monitoring.

3- Cox Communications' APIs were found to have significant security flaws, exposing over 700 endpoints, many of which provided administrative functionalities. These vulnerabilities allowed unauthorized access to sensitive customer information and device control.
Key Issues:

1. Exposed APIs: Many APIs were exposed without proper authentication and authorization checks, making them vulnerable to unauthorized access.
2. Information Disclosure: Attackers could retrieve full account PII, including device MAC addresses, email, phone numbers, and addresses, by exploiting the exposed APIs.
3. Device Control: The vulnerabilities allowed attackers to execute arbitrary commands, update device properties, and take over victim accounts by replaying HTTP requests.

Example Attack Scenario:

1. Identify a Cox business target using exposed APIs with their name, phone number, email, or account number.
2. Retrieve their full PII and device details.
3. Query hardware MAC addresses to retrieve WiFi passwords and connected devices.
4. Execute arbitrary commands to manipulate device settings and take over accounts.

Mitigation: Cox patched the vulnerabilities by restricting non-essential business endpoints, returning 403 errors to unauthorized requests, and began a comprehensive security review to prevent future occurrences.

4- A remote code execution (RCE) vulnerability was identified in Progress® Telerik® Report Server versions prior to 2024 Q1 (10.0.24.130), caused by insecure deserialization of untrusted data.
Root Cause: The vulnerability stems from the deserialization of untrusted data without proper validation, allowing attackers to execute arbitrary code on the server.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- CVE-2024-27348 (RCE) - Unauth users can execute commands via Groovy injection in Apache HugeGraph-Server
- Snowflake
- event log system in Windows
- Cox Communications' APIs
- Insecure Deserialization Vulnerability in Telerik Report Server
- CVE-2024-24919

🚨 Vulnerability of the Week

CheckPoint CVE-2024-24919

Active network exploitation of CVE-2024-24919 has been detected. This vulnerability, which affects Checkpoint Security Gateways solutions with Remote Access VPN (IPSec) or Mobile Access blade capabilities enabled, could allow a remote malicious user to steal sensitive information and gain access to target accounts. The vendor has already remediated this issue.
Estimated Impact: SERIOUS/RED (78.07/100)
Typology

- Information Disclosure
- Security Restrictions Bypass

The CVE-2024-24919 vulnerability exists in Checkpoint Security Gateways solutions with Remote Access VPN or Mobile Access blade functionality enabled. Exploitation of this vulnerability has been detected in the wild, despite the vendor having provided a remediation.
A remote unauthenticated attacker can leverage this vulnerability to:

- Disclose sensitive information
- Gain abusive access to VPN services, especially systems using passwords alone for authentication (notably local accounts)

Affected Products and Versions
The following products and versions are affected:

- 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

Mitigation and Recommendations

- Update and Patch: Ensure that your systems are updated to the latest versions as per the vendor's recommendations. Apply patches provided by Checkpoint immediately.
- Strengthen Authentication: Implement multi-factor authentication (MFA) wherever possible to reduce the risk posed by this vulnerability.
- Monitor and Audit: Continuously monitor network traffic and audit system logs for any unusual activity that could indicate exploitation attempts.
- Limit Exposure: Minimize the exposure of the affected systems to the internet. Restrict access to the VPN and Mobile Access blades to trusted IPs only.

Additional Resources

- CVE Details: CVE-2024-24919 on NVD
- Nuclei Template: CVE-2024-24919 Nuclei Template
- Shodan Dork: title:"Check Point" || "Server: Check Point SVN" "X-UA-Compatible: IE=EmulateIE7"
- Fofa Dork: app="Check_Point-SSL-Network-Extender"

Art of Detection

Sigma Log Source	Channel and EID	Default Settings	Rules	Percent
process_creation	Microsoft-Windows-Sysmon/Operational 1 or Security 4688	non-default	804	49.36%
security	Security	partial	139	8.53%
ps_script	Microsoft-Windows-PowerShell/Operational 4104	partial	125	7.67%
registry_set	Microsoft-Windows-Sysmon/Operational 13	sysmon	109	6.69%
file_event	Microsoft-Windows-Sysmon/Operational 11	sysmon	96	5.89%
system	System	default	50	3.07%
image_load	Microsoft-Windows-Sysmon/Operational 7	sysmon	39	2.39%
registry_event	Microsoft-Windows-Sysmon/Operational 12/13/14	sysmon	37	2.27%
ps_module	Microsoft-Windows-PowerShell/Operational 4103	non-default	30	1.84%
network_connection	Microsoft-Windows-Sysmon/Operational 3	sysmon	29	1.78%
process_access	Microsoft-Windows-Sysmon/Operational 10	sysmon	25	1.53%
pipe_created	Microsoft-Windows-Sysmon/Operational 17/18	sysmon	14	0.86%
application	Application	default	13	0.80%
dns_query	Microsoft-Windows-Sysmon/Operational 22	sysmon	12	0.74%
ps_classic_start	Windows PowerShell 400	default	10	0.61%
create_remote_thread	Microsoft-Windows-Sysmon/Operational 8	sysmon	10	0.61%

https://x.com/ptracesecurity/status/1797387763060273225

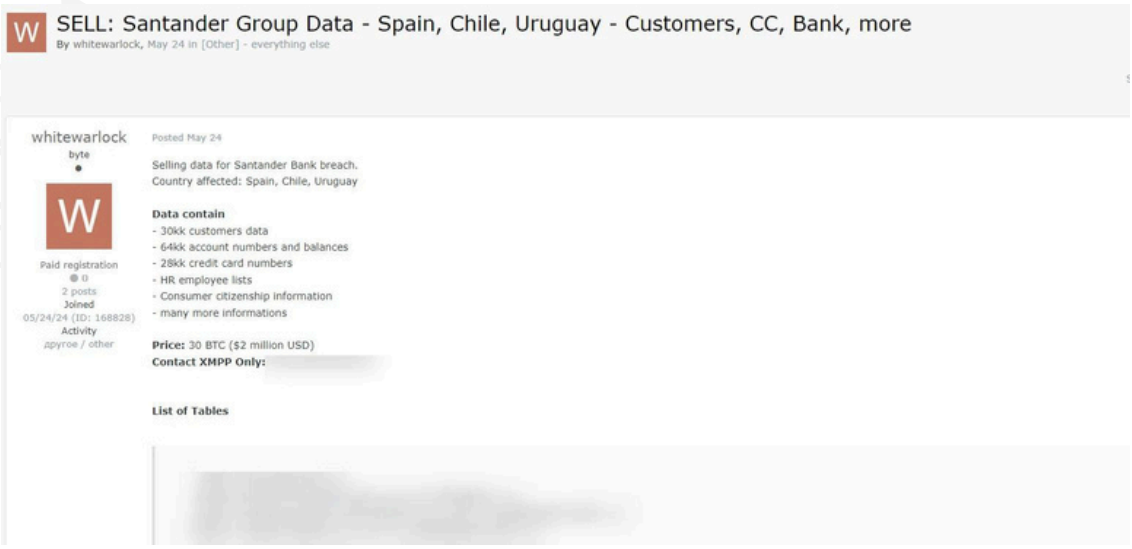
The event log system in Windows is crucial for tracking and analyzing various activities within the operating system. Event IDs provide detailed information about specific events, ranging from system startups and shutdowns to potential security threats. For example, Event ID 16 indicates when the registry hive access history is cleared, a potential sign of password dumping activities. Similarly, Event ID 55 highlights NTFS filesystem corruption, which could be indicative of attacks exploiting NTFS vulnerabilities. These events are classified with different levels of importance, from informational to critical, guiding administrators on which events require immediate attention.

In addition to the general system logs, specialized logs like the Application log and the Windows Defender Operational log provide more focused insights. The Application log, despite being noisy, can reveal critical events such as known vulnerability exploit attempts (Event ID 1) and application errors (Event IDs 1000, 1001). The Windows Defender Operational log is essential for monitoring alerts from Windows Defender, including tamper protection activities and the addition of exclusions, which are crucial for identifying and responding to security threats promptly.

Other specialized logs include the Bits-Client Operational log, which can detect misuse of the bitsadmin.exe tool by attackers to download and execute malware, and the Firewall log, which records changes to firewall rules. These logs help identify malicious activities such as the addition of firewall rules to facilitate communication with command-and-control servers. The NTLM Operational log is particularly important for environments looking to phase out NTLM authentication, as it allows administrators to monitor and gradually disable NTLM usage.

Logs such as the Security-Mitigations KernelMode and UserMode logs, PrintService logs, and SMBClient Security logs provide additional layers of security monitoring. For instance, the PrintService logs are useful for detecting Print Spooler attacks, while the SMBClient Security log helps identify suspicious SMB activities, such as rejected guest logons. The AppLocker logs and CodeIntegrity Operational logs are vital for enforcing application whitelisting and detecting malicious drivers, respectively. Collectively, these logs create a comprehensive system for monitoring, detecting, and responding to a wide range of security threats and system anomalies in a Windows environment.

😈 Malware or Ransomware



https://x.com/socradar/status/1797674964969230552

In recent weeks, Snowflake, a prominent cloud-based data storage and analytics provider, has been embroiled in a cybersecurity incident. Reports indicate that unauthorized access to its systems may have compromised sensitive data from high-profile clients, including Santander Bank and Ticketmaster. Snowflake, known for its robust data storage, processing, and analytics capabilities, is a key player in data-driven applications. This blog post will explore the details of the Snowflake breach, drawing on disclosures from Snowflake, news reports, and insights from cybersecurity researchers.

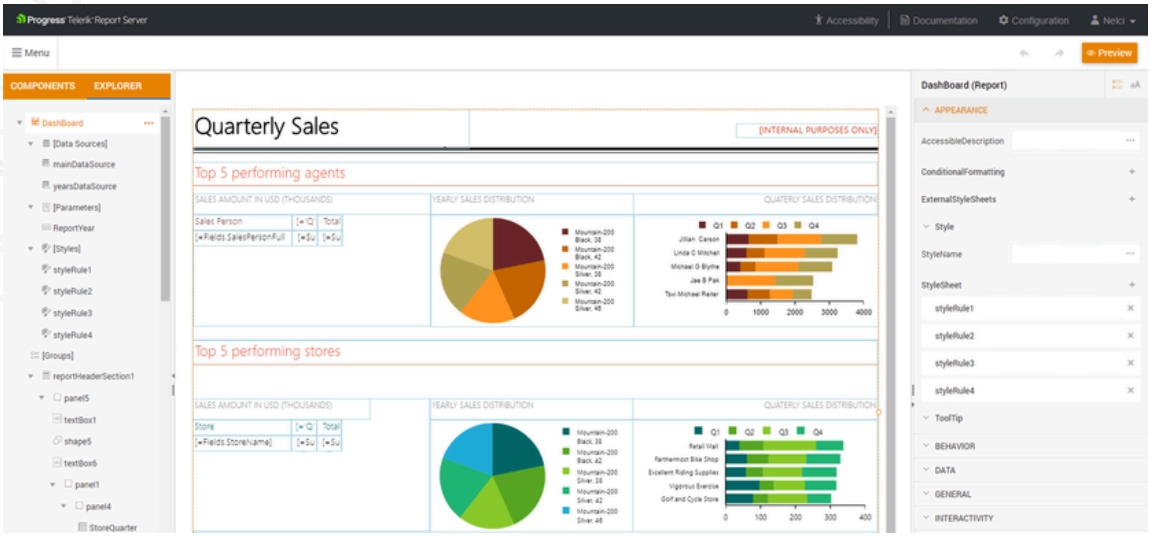
Snowflake first detected unusual activity in its systems around mid-April 2024 and officially acknowledged potential unauthorized access on May 23, 2024. The company has been investigating the situation and communicating with affected customers, providing Indicators of Compromise (IoCs) and recommended actions to secure their accounts. Despite allegations of a widespread breach, Snowflake asserts that the incidents were due to compromised user credentials rather than vulnerabilities in its product. The company emphasized that there was no misconfiguration or malicious activities within Snowflake's products, urging customers to review their security configurations.

Investigations into the breach suggest that it was facilitated by a compromised machine used by a Snowflake sales engineer, infected with Lumma Stealer malware. This malware logs keystrokes and other activities, likely serving as the initial access point for the attackers. The threat actor responsible claimed to have extracted sensitive data from major entities like Santander Bank and Ticketmaster. Following the breach, Santander Bank and Live Nation Entertainment (Ticketmaster's parent company) confirmed unauthorized access to databases hosted by a third-party provider, later linked to Snowflake's compromised environments. Cybersecurity firms conducted detailed analyses, revealing over 500 demo environment instances detected in the stealer logs related to the breach.

The threat actor behind the breach, known as "Whitewarlock," surfaced on a Russian dark web forum on May 23, 2024. They posted data allegedly obtained from the breach, including customers' data, account numbers and balances, credit card numbers, and HR employee lists from Santander Group. Whitewarlock claimed responsibility for the breach and demanded $2 million from Snowflake to return the stolen data. ShinyHunters, another threat actor group, also shared the same data to attract attention and further promote the Snowflake breach. Whitewarlock's sudden appearance and specific demands suggest an opportunistic attack rather than a coordinated campaign.

The broader impact of the breach is significant, with reports indicating that six major organizations have experienced cybersecurity issues related to their use of Snowflake. Security researcher Kevin Beaumont highlighted this on Mastodon, noting the extent of the breach's repercussions. Snowflake's proactive measures, including detailed communications with affected customers and ongoing investigations, aim to mitigate the breach's impact. The incident underscores the importance of stringent security practices and vigilant monitoring in safeguarding cloud-based environments from sophisticated cyber threats.

1Day



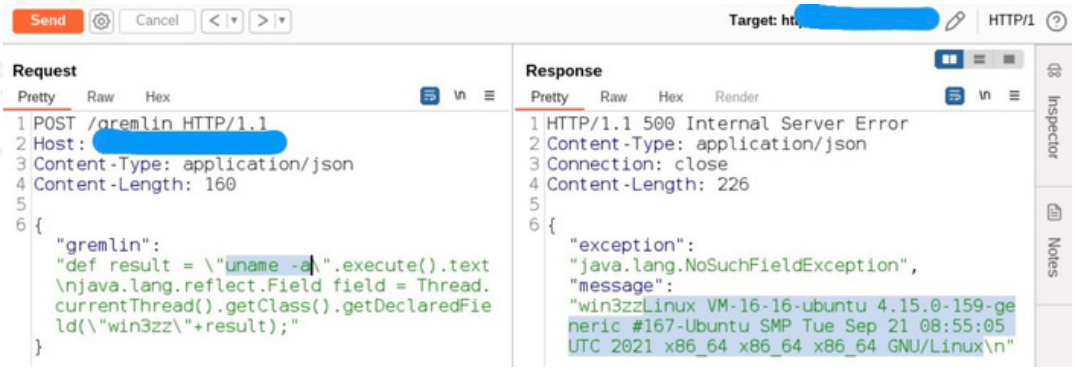
https://x.com/SinSinology/status/1797564978624692305

An insecure deserialization vulnerability has been identified in Progress® Telerik® Report Server versions prior to 2024 Q1 (10.0.24.130). This vulnerability can be exploited to execute remote code on the affected server.

The vulnerability arises from the insecure handling of serialized data in Report Server, allowing attackers to inject and execute arbitrary code remotely.

Updating to Report Server 2024 Q1 (10.0.24.305) or higher is the only way to eliminate this vulnerability.

NDay



https://x.com/adrielsec/status/1797307496408784921

CVE-2024-27348 is a critical remote code execution (RCE) vulnerability in Apache HugeGraph-Server. This flaw allows unauthorized users to execute arbitrary commands on the server through Groovy injection. The vulnerability affects versions of HugeGraph-Server from 1.0.0 to versions before 1.3.0. To mitigate this issue, users are advised to upgrade to version 1.3.0 or later.

A Python scanner has been developed to exploit this vulnerability, enabling ethical security professionals to test their systems for this specific issue. The scanner, available on GitHub (An insecure deserialization vulnerability has been identified in Progress® Telerik® Report Server versions prior to 2024 Q1 (10.0.24.130). This vulnerability can be exploited to execute remote code on the affected server.

The vulnerability arises from the insecure handling of serialized data in Report Server, allowing attackers to inject and execute arbitrary code remotely.

Updating to Report Server 2024 Q1 (10.0.24.305) or higher is the only way to eliminate this vulnerability.
), runs four commands (host, ping, curl, wget) on the target server to identify if the utilities are present and if the system is vulnerable. The scanner collects ping logs and DNS lookup/web request logs from the targets, which helps in determining if the commands were executed successfully.
The usage of the scanner is straightforward. It supports both single target and multiple target scanning modes. For single target scanning, the command is:

python3 CVE-2024-27348_Scanner.py -t http(s)://target_address -p port -d your_domain/ip

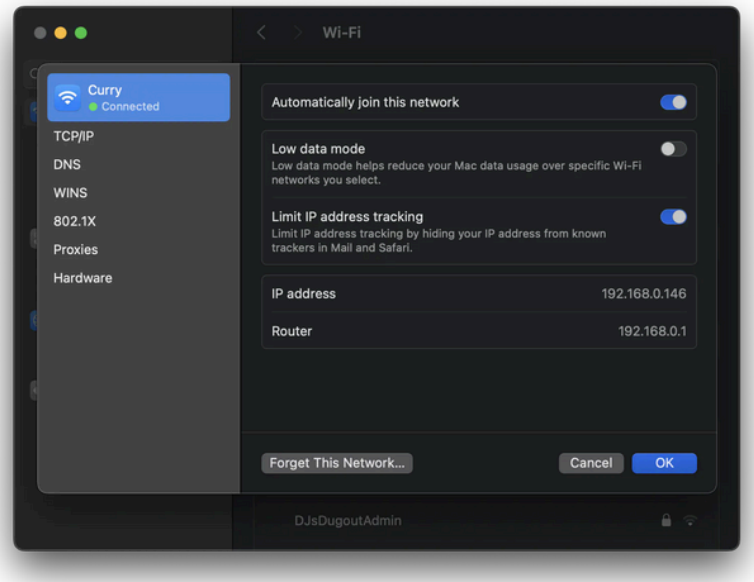
For scanning multiple targets listed in a file, the command is:

python3 CVE-2024-27348_Scanner.py -f targets_file -d your_domain/ip
The file should contain target addresses and ports in the format:

http://target,port

Security professionals can utilize this scanner to verify if their Apache HugeGraph-Server instances are vulnerable to CVE-2024-27348. Promptly upgrading to version 1.3.0 or later is essential to protect systems from potential exploitation. As with any security tool, it is crucial to ensure it is used responsibly and within legal and ethical boundaries.

The Topic of the Week



https://x.com/samwcyo/status/1797500342814507070

Two years ago, while working from my home network, I encountered a strange and alarming incident. During an exploit of a blind XXE vulnerability, I set up an AWS server to receive traffic and noticed an unknown IP address replaying my HTTP requests. To ensure this wasn't an anomaly, I repeated the test with different devices and new servers on AWS and GCP, all showing the same behavior. This led me to suspect that my modem or ISP had been compromised, although the unknown IP address was traced back to DigitalOcean.

Further investigation into the DigitalOcean IP revealed it had a history of being used for phishing and malicious activities, including targeting a South American cybersecurity company. The repeated interception and replay of my HTTP requests suggested a sophisticated level of network monitoring, likely through my ISP or modem. Despite reaching out to threat intelligence contacts and examining the data, the exact method of compromise remained unclear. The incident underscored the vulnerabilities inherent in the trust relationship between ISPs and customer devices.

In a related incident, I discovered significant vulnerabilities in Cox Communications' APIs, which allowed unauthorized access to customer PII and device control. After reporting these findings, Cox patched the vulnerabilities and began a comprehensive security review. However, they confirmed that my initial device compromise was unrelated to these newly found vulnerabilities. The exact mechanism of my modem's compromise remains a mystery, but the experience highlights the critical need for robust security measures and vigilant monitoring in protecting network infrastructures.

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Threat Radar
WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.