

Threat Intel Roundup: Outlook, QNAP, Okta



Week in Overview[5 Mar-12 Mar] - 2024



THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

- 1. How to Leverage Internal Proxies for Lateral Movement, Firewall Evasion, and Trust Exploitation:** This article explores techniques for utilizing internal proxies within a compromised network. It covers methods such as port forwarding using netsh and custom TCP proxies, highlighting their applications in lateral movement, firewall evasion, and trust exploitation.
- 2. Okta Denies Alleged Data Leak Following Cyberattack Claims:** Okta refutes claims of a data breach after threat actor 'Ddarknotevil' purportedly shared files stolen during a 2023 cyberattack on a hacker forum. Okta asserts the data does not belong to them, suggesting it may be from a different breach.
- 3. Introducing Misconfiguration Manager: A Repository for Securing Microsoft Configuration Manager:** Researchers release Misconfiguration Manager, a repository focusing on attack and defense techniques related to improperly configured Microsoft Configuration Manager instances. The repository aims to educate on securing Configuration Manager against potential vulnerabilities.

- 4. Critical Security Alert: CVE-2024-1403 in Progress OpenEdge:** CVE-2024-1403, a critical vulnerability in Progress OpenEdge, allows unauthorized users to obtain admin permissions and potentially execute remote code. While no path to Remote Code Execution (RCE) has been discovered, the exploit poses significant risks.
- 5. Urgent Security Alert: CVE-2024-21899 Exploits Targeting QNAP NAS Systems:** QNAP NAS systems face exploitation via CVE-2024-21899, which includes an authentication bypass vulnerability and other critical flaws. Attackers could compromise affected devices, emphasizing the importance of immediate updates to patched versions.
- 6. Unraveling Latrodectus: A Sophisticated Malware Campaign:** An analysis of the Latrodectus malware campaign reveals its complex attack chain, involving URL redirection, malicious JavaScript, SMB, MSI, and DLL files. The campaign's infrastructure, indicators of compromise (IOCs), and samples are detailed.
- 7. Unveiling a Critical Vulnerability in Microsoft Outlook: CVE-2024-21378:** CVE-2024-21378 exposes a critical vulnerability in Microsoft Outlook, potentially allowing attackers to execute arbitrary code. The vulnerability affects Outlook's handling of certain email content, posing significant security risks to users.

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:

- How to Leverage Internal Proxies for Lateral Movement, Firewall Evasion, and Trust Exploitation
- Okta Denies Alleged Data Leak Following Cyberattack Claims
- A Repository for Securing Microsoft Configuration Manager
- CVE-2024-1403 in Progress OpenEdge
- CVE-2024-21899 Exploits Targeting QNAP NAS Systems
- A Sophisticated Malware Campaign
- Unveiling a Critical Vulnerability in Microsoft Outlook: CVE-2024-21378



Vulnerability of the Week

Outlook CVE-2024-21378

In the ever-evolving landscape of cybersecurity threats, 2023 saw a significant revelation by NetSPI regarding a critical vulnerability lurking within Microsoft Outlook. This vulnerability, designated CVE-2024-21378, opened the doors to authenticated remote code execution (RCE) via synced form objects. In this exposé, we delve into the discovery of this flaw and its subsequent weaponization, utilizing modifications to Ruler, an Outlook penetration testing tool initially published by SensePost. It's crucial to note that a pull request containing proof-of-concept code is on the horizon, ensuring organizations have adequate time to patch their systems.

The Vulnerability Unveiled

The genesis of this vulnerability traces back to an original attack variant outlined by Etienne Stalmans at SensePost (Orange CyberDefense) in 2017. This exploit relied on VBScript code embedded within Outlook form objects, facilitating code execution with mailbox access. Although a patch was issued in response, mandating allowlisting for script code in custom forms, the syncing capability of these form objects remained unchanged. Beneath the surface, forms are MAPI synced using `IPM.Microsoft.FolderDesign.FormsDescription` objects, housing special properties and attachments crucial for form installation on clients. The vulnerability stems from flaws in this installation process:

- 1. Arbitrary Disk Write:** Path traversal via the `PidTagAttachFilename` property enables arbitrary file creation on disk during form installation.
- 2. Registry Manipulation:** Manipulating registry keys under `HKEY_CLASSES_ROOT (HKCR)` during form installation allows for arbitrary registry modifications, a potent vector for RCE.

In-Depth Analysis

This discovery marks the culmination of a series of attacks leveraging compromised credentials to sync objects through Exchange. Beginning with Nick Landers' 2015 revelation on the exploitation of Outlook Rules for RCE, subsequent discoveries by Etienne at SensePost and Nick uncovered additional vectors, ultimately patched by Microsoft. SensePost's comprehensive blogs delved into these vulnerabilities and the underlying technologies, alongside the exploitation tool, Ruler.

Our foray into this research was spurred by the vast, yet underexplored attack surface presented by Outlook. Leveraging insights gained from engagements utilizing Device Code phishing/vishing, we embarked on a meticulous exploration of Outlook forms, employing tools like MFCMAPI and ProcMon to dissect the underlying technology.

Exploitation and Verification

Our journey began with attempts to demonstrate local code execution. Crafting a custom form configuration file, we imported it into Outlook to install a form, effectively setting the stage for exploitation. Through iterative testing, we confirmed the execution of arbitrary DLLs, a pivotal milestone in our exploit development.

Further exploration via MFCMAPI provided deeper insights into the workings of Outlook, unraveling the mechanics of form installation and storage within the system. This meticulous analysis unveiled the extent of the vulnerability, showcasing the potential for not just code execution but also arbitrary registry writes and file manipulation, all from within the confines of Outlook.

<https://twitter.com/NetSPI/status/1767175389569290359>



Art of Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
PXE Credentials	App Deployment	App Deployment	Relay to Site Server SMB	App Deployment	PXE Credentials	LDAP Enumeration	App Deployment	CMPivot		CMPivot
	Script Deployment	Script Deployment	Relay Client Push Installation	Script Deployment	Policy Request Credentials	SMB Enumeration	Script Deployment			
		ADCS Relay	Relay to DB MSSQL		DPAPI Credentials	HTTP Enumeration	Relay to Site Server SMB			
		LDAP Relay	Relay to DB SMB		Legacy Credentials	CMPivot	Relay Client Push Installation			
			Relay to ADCS				Relay to DB MSSQL			
			Relay to AdminService		Site Database Credentials		Relay to DB SMB			
			Relay CAS to Child				Relay CAS to Child			
			Relay to SMS Provider SMB				Relay to AdminService			
			Relay between HA				Relay to SMS Provider SMB			

<https://twitter.com/SpecterOps/status/1767288177797038459>

Security researchers at SpecterOps have unveiled Misconfiguration Manager, a comprehensive knowledge base repository designed to address the vulnerabilities stemming from improperly configured instances of Microsoft's Configuration Manager (MCM). This initiative aims to equip both defenders and offensive security professionals with the necessary tools and insights to bolster security and mitigate potential risks associated with MCM deployment.

Understanding Microsoft Configuration Manager (MCM)

Formerly known as System Center Configuration Manager (SCCM, ConfigMgr), MCM has been a staple in Active Directory environments since 1994, serving as a crucial tool for administrators to manage servers and workstations within Windows networks. However, its extensive capabilities also make it a prime target for security research and exploitation, with adversaries seeking to leverage misconfigurations to gain unauthorized access and administrative privileges.

The Need for Misconfiguration Management

The complexity of MCM configurations often leaves room for vulnerabilities, with default settings and practices inadvertently exposing systems to potential exploitation. As highlighted by SpecterOps researchers Chris Thompson and Duane Michael, common misconfigurations such as overly privileged network access accounts (NAAs) can pave the way for attackers to escalate privileges and compromise critical components within the environment.

Attack Scenarios and Risks

The release of Misconfiguration Manager sheds light on various attack scenarios and risks associated with improperly configured MCM deployments. From compromising SharePoint accounts to achieving domain controller status, attackers can exploit vulnerabilities in MCM to execute payloads, elevate privileges, and infiltrate the network. Examples provided by Michael underscore the severity of these risks, emphasizing the need for proactive defense measures.

Empowering Defenders and Offensive Professionals

The Misconfiguration Manager repository, curated by Thompson, Garrett Foster, and Duane Michael, serves as a comprehensive resource for administrators, offering insights into MCM attack vectors and defensive strategies. With 22 techniques outlined, defenders can gain a deeper understanding of potential vulnerabilities and take proactive steps to mitigate risks. Additionally, offensive professionals can leverage this repository to enhance their knowledge of MCM's attack surface and refine their penetration testing strategies.

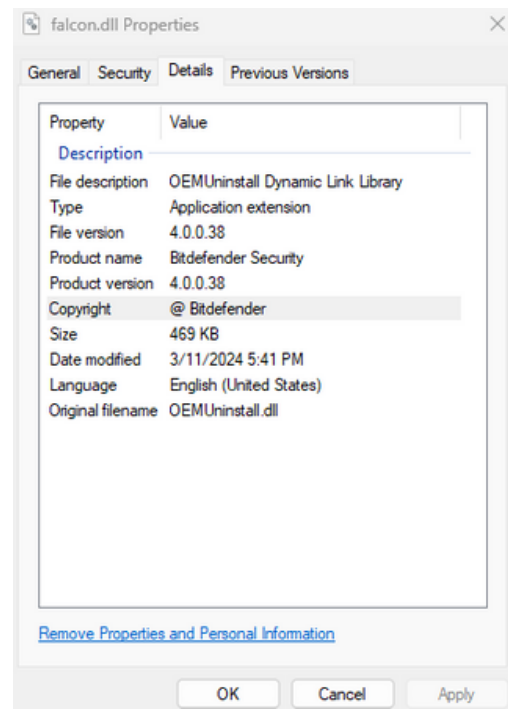
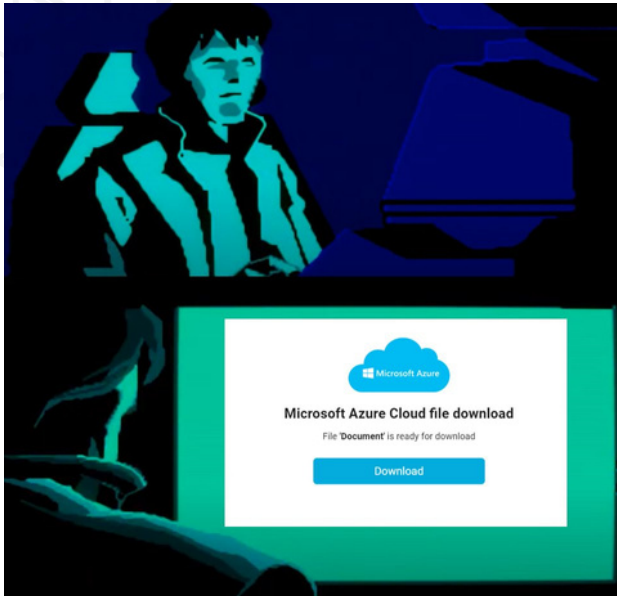
Defense Strategies: PREVENT, DETECT, CANARY

The repository categorizes defense actions into three key areas:

- **PREVENT:** Configuration changes aimed at directly mitigating or impacting attack techniques.
- **DETECT:** Guidance and strategies for detecting various attack techniques within the environment.
- **CANARY:** Detection strategies based on deception, utilizing features commonly abused by attackers.



Malware or Ransomware



<https://twitter.com/Cryptolaemus1/status/1767303559689736264>

The cybersecurity landscape is often fraught with sophisticated threats, and the emergence of Latrodectus exemplifies this paradigm shift. This clandestine campaign operates through a meticulously orchestrated sequence, leveraging a series of stages encompassing URL manipulation, JavaScript execution, SMB exploitation, MSI installation, and DLL payload execution. In this narrative, we dissect the modus operandi of Latrodectus, shedding light on its intricacies and implications.

Initial Entry: URL Manipulation and JavaScript Execution

The inception of Latrodectus typically begins with the manipulation of URLs, luring unsuspecting users into accessing malicious JavaScript (.js) files. These files, often disguised as innocuous content, serve as the conduit for initiating the malware deployment chain. Upon execution via tools like **wscript**, these JavaScript payloads initiate the next phase of the attack.

SMB Exploitation and MSI Installation

Once the JavaScript payload is executed, Latrodectus proceeds to exploit vulnerabilities within the Server Message Block (SMB) protocol. By leveraging SMB, the malware establishes a connection to a remote server, facilitating the retrieval of malicious .msi (Windows Installer) files. These MSI files, typically embedded within the JavaScript payload or retrieved from remote locations, serve as the vehicle for deploying the malware onto the victim's system.

DLL Payload Execution

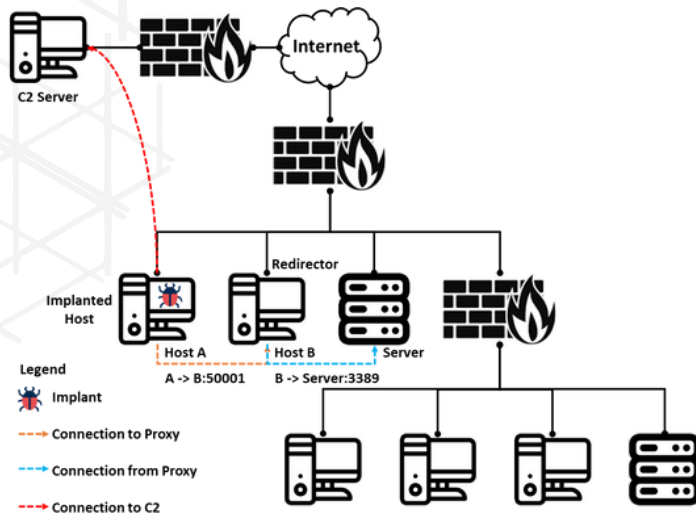
With the MSI files successfully retrieved, Latrodectus proceeds to execute the embedded DLL payloads. Utilizing system utilities like **msiexec.exe**, the malware silently installs these DLLs onto the victim's system, often within temporary directories to evade detection. Once installed, these DLLs are invoked for execution through system utilities like **rundll32.exe**, unleashing their malicious payloads.

Indicators of Compromise (IOCs) and Command & Control (C2) Infrastructure

As with any sophisticated malware campaign, Latrodectus leaves behind a trail of indicators of compromise (IOCs) and operates through a network of command and control (C2) infrastructure. These IOCs, meticulously documented by security researchers, provide crucial insights into the behaviors and characteristics of the malware. Additionally, the C2 infrastructure serves as the linchpin for orchestrating and coordinating malicious activities, encompassing a network of domains and servers.



TTP Analysis



This post explores the utilization of internal proxies within a target network for various purposes such as lateral movement, firewall evasion, trust exploitation, and defense evasion. We'll delve into techniques using tools like PowerShell, netsh, and SpecterInsight.

Techniques:

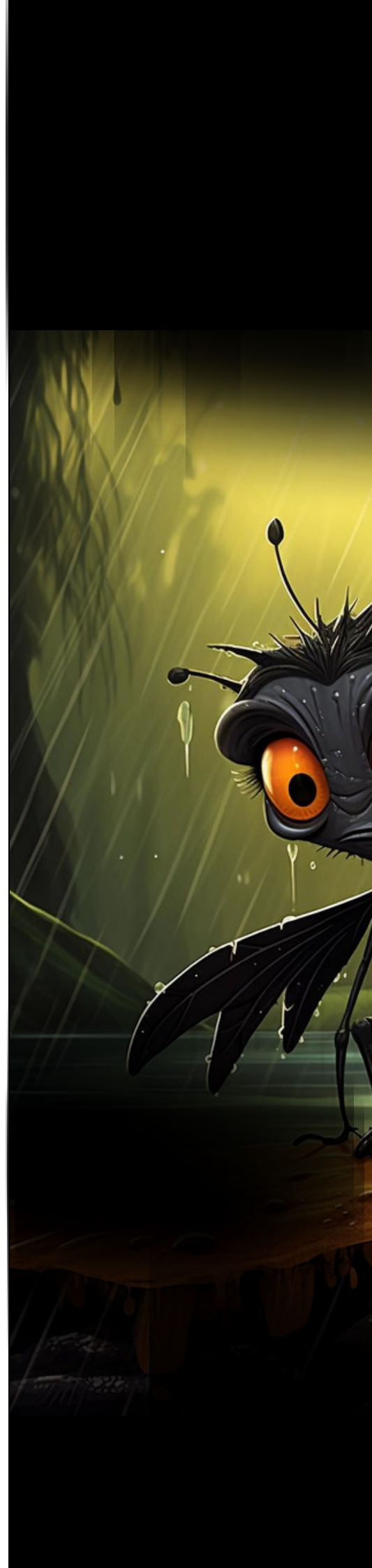
- Internal Scanning:** Utilize port proxies to scan internal network services, minimizing the risk of detection.
- Lateral Movement:** Employ port proxies to facilitate lateral movement within the network, often evading detection mechanisms.
- Firewall Evasion:** Use port proxies to bypass firewalls and other network security controls, enabling persistent communication.
- Trust Exploitation:** Leverage port proxies to exploit trust relationships between systems, facilitating lateral movement.
- Defense Evasion:** Evade detection mechanisms, such as Endpoint Detection and Response (EDR) systems, by separating the C2 callout process from the implant process using port proxies.

Netsh Interface Portproxy:

- Description:** Configure port forwarding and proxying for network connections using netsh.
- Employment Considerations:**
 - Windows-only technique.
 - Requires high integrity or SYSTEM process for execution.
 - Can evade certain detection analytics by using a separate process for network connections.
 - No custom code required, making it a live-off-the-land technique.

TCP Proxy Using Implant Modules:

- Description:** Load custom code into a process controlled by the attacker to establish a TCP proxy.
- Employment Considerations:**
 - Works on any operating system.
 - Can be run from any process integrity level.
 - Requires a firewall exemption.
 - May trigger network permission prompts depending on the process.





1Day

```
← → ↻ 🏠 54.145.48.76:3000/api/cors/http/169.254.169.254/latest/meta-data
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hibernation/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
system
```

<https://twitter.com/Horizon3Attack/status/176718627925336485>

A critical vulnerability, CVE-2024-1403, has been uncovered in Progress OpenEdge, posing significant security risks to affected systems. This authentication bypass flaw enables unauthorized users to gain administrative privileges, potentially allowing them to manipulate services within the environment. While a direct path to Remote Code Execution (RCE) has not been confirmed, the severity of this vulnerability demands immediate attention and remediation efforts.

Overview of CVE-2024-1403:

The essence of CVE-2024-1403 lies in an authentication bypass mechanism within Progress OpenEdge. Specifically, if the username matches the string "NT AUTHORITY/SYSTEM," the system grants administrative permissions, bypassing the authentication process. This loophole effectively grants unauthorized users elevated privileges, compromising the integrity and security of the system.

Risk Implications:

The implications of CVE-2024-1403 are grave. With administrative access, attackers can exert control over critical services within the Progress OpenEdge environment. This could lead to unauthorized data access, manipulation, or even disruption of essential business operations. Furthermore, while a direct path to Remote Code Execution has not yet been confirmed, the nature of the vulnerability suggests that such an exploit may be feasible, further exacerbating the risk landscape.

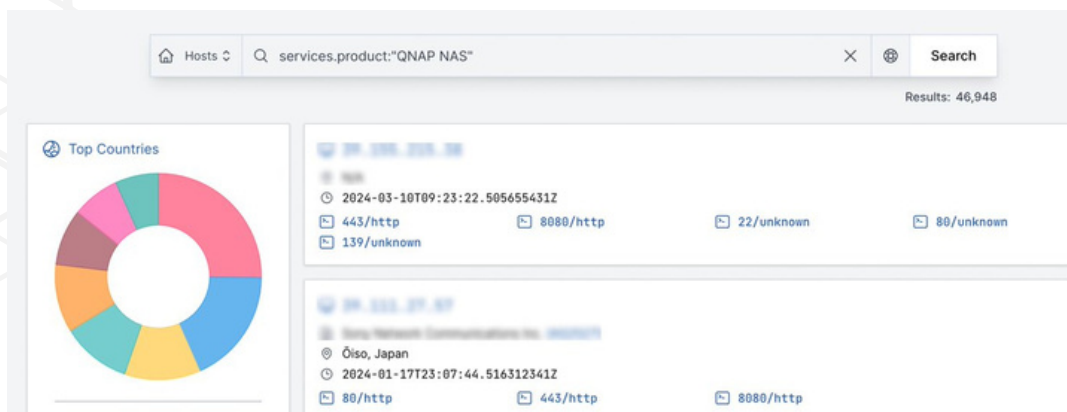
Research and Exploit Details:

A comprehensive analysis of CVE-2024-1403 has been conducted by security researchers at Horizon3 AI, providing valuable insights into the vulnerability and its potential impact. Their deep dive into the exploit, along with a detailed write-up, sheds light on the technical intricacies of the flaw. Additionally, an exploit for CVE-2024-1403 has been made publicly available on GitHub, underscoring the urgency of addressing this vulnerability.





Trending Exploit



<https://twitter.com/OdinThreatIntel/status/1767117992306045113>

In a recent security advisory, QNAP has disclosed critical vulnerabilities affecting their NAS (Network Attached Storage) software solutions. These vulnerabilities pose significant risks, potentially enabling attackers to compromise affected devices and gain unauthorized access to sensitive data. Below is an overview of the identified vulnerabilities and recommended actions to mitigate the associated risks:

CVE-2024-21899: Authentication Bypass (CVSS 9.8)

The most critical vulnerability identified is an authentication bypass flaw (CVE-2024-21899), allowing attackers to remotely access QNAP NAS devices without requiring valid credentials. Exploiting this flaw requires minimal effort and could lead to unauthorized access to sensitive data stored on the device.

Other Vulnerabilities Identified:

- CVE-2024-21900 (CVSS 4.3): Command Injection vulnerability enabling authenticated users to execute arbitrary commands.
- CVE-2024-21901 (CVSS 4.7): SQL Injection vulnerability allowing authenticated users to compromise the integrity of the device's database.
- CVE-2023-32969 (CVSS 4.9): Cross-Site Scripting (XSS) vulnerability impacting Network & Virtual Switch, potentially enabling authenticated administrators to execute malicious code.

Affected Systems:

These vulnerabilities impact various QNAP operating systems, including:

- QTS 5.1.x
- QTS 4.5.x
- QuTS hero h5.1.x
- QuTS hero h4.5.x
- QuTScldoud c5.x
- myQNAPcloud 1.0.x service

Recommended Actions:

QNAP strongly advises users to apply immediate updates to patched versions, including:

- QTS 5.1.3.2578 build 20231110 and later
- QTS 4.5.4.2627 build 20231225 and later
- QuTS hero h5.1.3.2578 build 20231110 and later
- QuTS hero h4.5.4.2626 build 20231225 and later
- QuTScldoud c5.1.5.2651 and later
- myQNAPcloud 1.0.52 (2023/11/24) and later

Updating is straightforward; administrators can navigate to the 'Control Panel > System > Firmware Update' pathway for QTS, QuTS hero, and QuTScldoud systems. Meanwhile, myQNAPcloud users can utilize the 'App Center' to locate and update their software.




The Topic of the Week

Okta Database, Leaked - Download!
by Ddarknotevil - Saturday March 9, 2024 at 06:43 AM

03-09-2024, 06:43 AM #1

Ddarknotevil




Thank me later

GOD

Posts: 345
Threads: 169
Joined: Aug 2023
Reputation: 842

Hello BreachForums Community.
Today, I have uploaded the [Okta database](#) for you all, This Breach is being shared in behife @[IntelBroker](#) - [Cyber] thanks for reading and enjoy!



In September 2023, Okta, an IT service management company, suffered a data breach that led to the exposure of 3.8 thousand customer support users.
User Compromised data:

User ID	First Name	Last Name	Username	Company Name	Company Title
Address	Time Zone	ID	DST Flag	Phone: Office	Phone: Home
Cell	Default Email	Other Email(s)	Security Parameter	Account	
Status	Last Login	Notes	Roles	Groups	

<https://twitter.com/BleepinComputer/status/1767283526028640587>

Okta, a leading cloud identity and access management solutions provider based in San Francisco, has refuted claims of a data breach after a threat actor purportedly shared files allegedly pilfered during an October 2023 cyberattack on a hacker forum.

In October 2023, Okta disclosed a security incident where its support system was compromised by hackers wielding stolen credentials. This breach facilitated the theft of cookies and authentication data for select customers. Subsequent internal investigations revealed that the incident impacted all users of the customer support system, raising concerns about potential breaches for multiple Okta clients. Notably, hackers utilized access tokens pilfered during the Okta breach to compromise one of Cloudflare's self-hosted Atlassian servers.

Over the weekend, a cybercriminal under the pseudonym 'Ddarknotevil' claimed to have leaked an Okta Database containing information of 3,800 customers allegedly stolen during the 2023 breach. The leaked data purportedly includes user IDs, full names, company names, office addresses, phone numbers, email addresses, positions/roles, and other information.

Upon reaching out to Okta for clarification, the company promptly denied any association with the leaked data. An Okta spokesperson emphasized that the data does not belong to Okta and appears to be sourced from publicly available information on the internet. Despite claims made by the threat actor, Okta's IT team conducted thorough investigations over the weekend and found no evidence of a breach within their systems.

Further analysis conducted by cyber-intelligence firm KELA supported Okta's assertion, confirming that the shared data does not originate from Okta. Instead, KELA identified the data as matching a dump from a separate breach in July 2023, attributed to the threat actor 'IntelBroker.' The data was purportedly stolen from the National Defense Information Sharing and Analysis Center during the July breach.

In light of these developments, Okta reassures its customers of its commitment to maintaining robust security measures and continues to monitor its systems vigilantly to safeguard against potential threats. Despite the false alarm, the incident underscores the importance of proactive cybersecurity measures and swift response protocols in today's digital landscape.



cat /etc/HADESS

"Hades" 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