Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Hackers Exploit Ivanti vTM Flaw to Create Rogue Admin Accounts

Date of Publication	Last Update Date	Admiralty Code	TA Number
August 14, 2024	September 27, 2024	A1	TA2024311

Summary

First Seen: August 2024
Affected Products: Ivanti Virtual Traffic Manager (vTM)
Impact: Ivanti has identified a critical authentication bypass vulnerability, designated as CVE-2024-7593, affecting their Virtual Traffic Manager (vTM) appliances. This flaw enables attackers to potentially create unauthorized administrator accounts, significantly increasing the risk of unauthorized access and control over affected systems. With a proof of concept now publicly available, it is imperative that customers upgrade to the latest patched version to mitigate this risk.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-7593	Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability	Ivanti Virtual Traffic Manager (vTM)	✗	✓	✓

Vulnerability Details

#1 A critical vulnerability has been identified in Ivanti Virtual Traffic Manager (vTM), designated as CVE-2024-7593. This flaw enables authentication bypass, allowing attackers to exploit it to create unauthorized administrative accounts.

#2 Ivanti vTM is a software-based application delivery controller (ADC) designed to manage, optimize, and secure application traffic across both data centers and cloud environments. It provides advanced traffic management capabilities, including load balancing, SSL/TLS termination, content caching, and application acceleration.

#3 This vulnerability allows an unauthenticated remote attacker to bypass the admin panel authentication and execute malicious actions on Ivanti vTM. Additionally, it enables the attacker to create an administrator account on compromised Ivanti instances. The flaw stems from a flawed implementation of the authentication algorithm in Ivanti vTM.

#4 As a temporary mitigation, Ivanti recommends that customers restrict admin access to the management interface or limit access to trusted IP addresses. While there is no evidence of the vulnerability being actively exploited in the wild, Ivanti acknowledges the public availability of a proof-of-concept (PoC). Therefore, it is critical for users to apply the latest patches promptly to address the issue.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7593	Ivanti Virtual Traffic Manager Versions: 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, 22.7R1	cpe:2.3:a:ivanti:vtm:*:*:*:*:*:*:*	CWE-287, CWE-303

Recommendations

Apply Patch: Users should apply the available patches by upgrading to the latest version of Ivanti vTM. These security patches specifically address the flaw and help protect against potential exploits. Upgrading ensures that your system is safeguarded from this vulnerability and other related security risks.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Limit Exposure: Restrict access to critical systems and endpoints to minimize potential attack vectors. Implement strict network access controls to ensure that only authorized users and systems can interact with sensitive components.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0004** Privilege Escalation	**TA0006** Credential Access
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation
T1556 Modify Authentication Process			

Patch Details

Users are urged to apply the available patches by upgrading to the latest version of Ivanti vTM.
Fixed Versions: Ivanti Virtual Traffic Manager 22.2R1, 22.3R3, 22.5R2, 22.6R2, 22.7R2.

Patch Link:
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593

Workaround: User can limit admin access to the management interface by restricting it to the internal network through the private or corporate network, thereby reducing the exploitability of this vulnerability. To implement this, go to System > Security on the vTM server, select Management IP Address and Admin Server Port, and choose the Management Interface IP Address from the bindip drop-down menu.

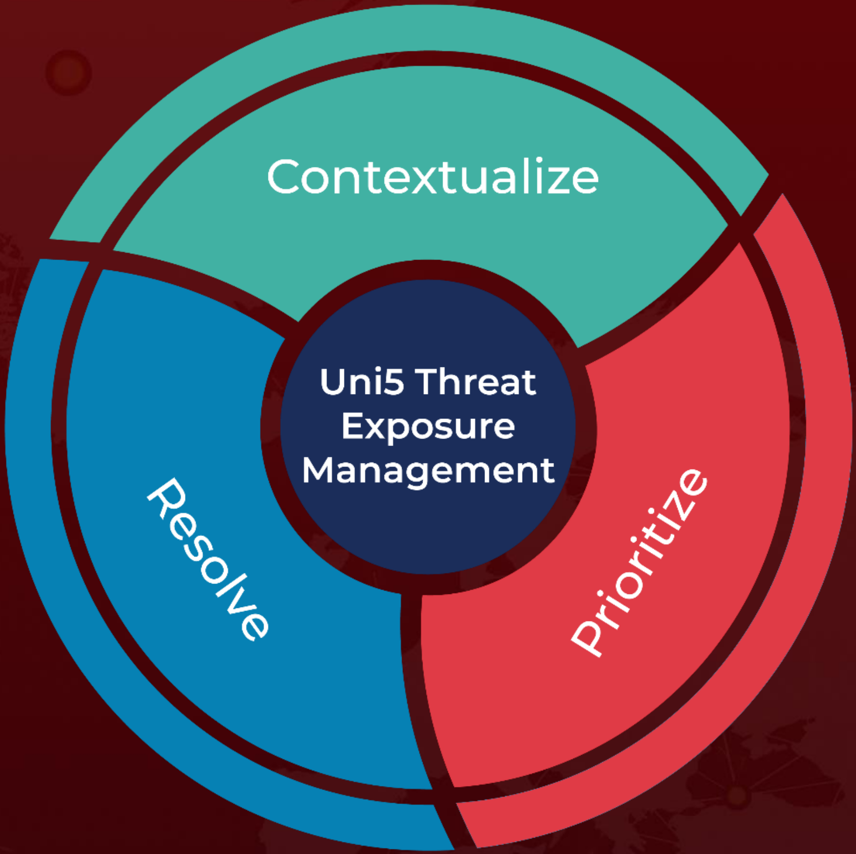
References

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 14, 2024 • 6:15 AM

More at www.hivepro.com