Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Chinese Hackers Leverage Cityworks Bug to Take Over Vital Systems

Date of Publication

May 23, 2025

Admiralty Code

A1

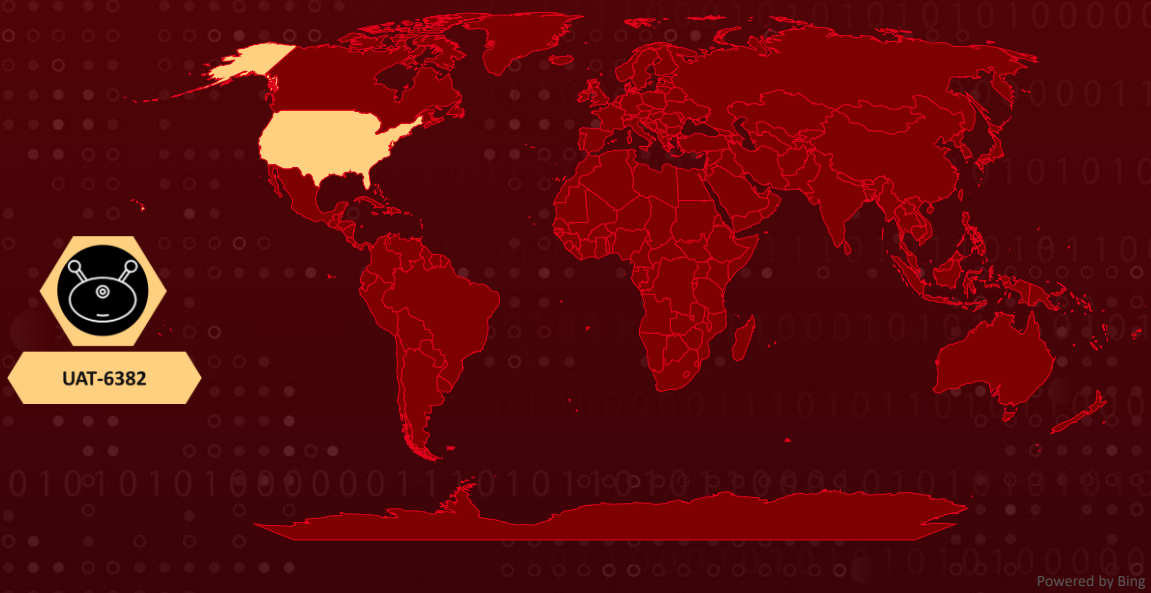
TA Number

TA2025162

Summary

Attack Commenced: January 2025
Threat Actor: UAT-6382
Malware: TetraLoader
Targeted Country: United States
Targeted Industry: Government
Affected Product: Trimble Cityworks
Attack: The Chinese-speaking threat actor UAT-6382 exploited CVE-2025-0994, a zero-day vulnerability in Trimble Cityworks, enabling remote code execution, conducting targeted reconnaissance, and deploying custom malware for persistent access within critical infrastructure networks. Unpatched systems remain at high risk of similar attacks and operational disruption.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0994	Trimble Cityworks Deserialization Vulnerability	Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10	✓	✓	✓

Attack Details

#1 In January 2025, a Chinese-speaking threat actor identified as UAT-6382 successfully exploited CVE-2025-0994, a deserialization vulnerability in Trimble Cityworks. This flaw allows authenticated users to execute remote code on affected systems.

#2 Cityworks is a widely used asset and work order management platform, particularly popular among critical infrastructure sectors such as water utilities, energy providers, transportation systems, and government services. Following the initial intrusion, the attackers took advantage of this vulnerability to conduct extensive reconnaissance, identifying and targeting networks associated with utility management.

#3 They then deployed malicious tools to steal sensitive files and maintain long-term, covert access to these environments. A key component of their toolkit was a custom loader known as TetraLoader, built using MaLoader, a malware framework written in Simplified Chinese.

#4 TetraLoader enables operators to encapsulate shellcode and other payloads within Rust-based binaries, allowing the attackers to discreetly deploy advanced tools while evading detection. If left unaddressed, this vulnerability poses a serious risk to organizations that rely on Cityworks, potentially exposing them to similar attacks that could disrupt operations, compromise sensitive data, and threaten public services.

Recommendations

Apply Security Updates Without Delay: To mitigate the risks associated with CVE-2025-0994, all on-premise Cityworks users should immediately apply the security updates: version 15.8.9 and version 23.10. These updates address a critical remote code execution vulnerability actively exploited in recent attacks. While Cityworks Online (CWOL) deployments will receive these updates automatically, on-premise environments must proactively install them to prevent potential compromise.

Audit and Restrict IIS Identity Permissions: Review on-premise Internet Information Services (IIS) identity permissions to ensure they do not run with local or domain-level administrative privileges. This configuration is critical to limiting potential lateral movement in the event of a compromise.

Secure Attachment Directory Configurations: Verify that attachment directory root configurations are restricted exclusively to folders or subfolders containing attachments. Inappropriate configurations can increase the risk of unauthorized file access and malware staging.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0008** Lateral Movement	**TA0011** Command and Control	**TA0010** Exfiltration
T1059 Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1059.001** PowerShell	**T1505** Server Software Component
T1505.003 Web Shell	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1027** Obfuscated Files or Information
T1083 File and Directory Discovery	**T1082** System Information Discovery	**T1021** Remote Services	**T1021.001** Remote Desktop Protocol
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1074** Data Staged	**T1041** Exfiltration Over C2 Channel
T1587 Develop Capabilities	**T1587.001** Malware	**T1588** Obtain Capabilities	**T1588.005** Exploits
T1505.004 IIS Components	**T1588.006** Vulnerabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	14ed3878b6623c287283a8a80020f68e1cb6bfc37b236f33a95f3a64c4f4611f, 4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9, 1de72c03927bcd2810ce98205ff871ef1ebf4344fba187e126e50caa1e43250b, 1c38e3cda8ac6d79d9da40834367697a209c6b07e6b3ab93b3a4f375b161a901, c02d50d0eb3974818091b8dd91a8bbb8cdefd94d4568a4aea8e1dcdd8869f738, 4b7561e27c87a1895446d7f2b83e2d9fcf71e6d6e8bc99d44818dc39a6ff99d5, 8a6c735f3608719ec9f46d9c6c5fc196db8c97065957c218b98733a491edd899, 883d849b94238c26c57c0595ccb95b8c356628887b9a3628bf56e726332af925, 151a71c43e63db802d41d5d715aa98eb1b236e0a6441076a8d30fd93990416b4, 14a072113baa0a1e1e2b6044068c7bc972ae5e541a0aec06577b0d6663140079, 04dc3a16e1e2b4924943805a1cea5e402c4f2304c717ea21fdf43274b8c34a84, f09b51b759dfe7de06fa724bd89592f5b8eae57053d5fb4891e40f24055103fb
IPv4	23[.]247[.]136[.]238, 31[.]59[.]70[.]13, 31[.]59[.]70[.]11, 149[.]112[.]117[.]49, 192[.]210[.]137[.]81, 192[.]210[.]183[.]118, 192[.]210[.]239[.]172
Domains	cdn[.]phototagx[.]com, www[.]roomako[.]com, lgaircon[.]xyz, ifode[.]xyz
URLs	hxxps[:]//www[.]roomako[.]com/jquery-3[.]3[.]1[.]min[.]js, hxxps[:]//lgaircon[.]xyz/owa/OPWiaTU-ZEbuwIAKGPHoQAP006-PTsjBGKQUxZorq2, hxxps[:]//cdn[.]lgaircon[.]xyz/jquery-3[.]3[.]1[.]min[.]js, hxxps[:]//cdn[.]phototagx[.]com/, hxxp[:]//192[.]210[.]239[.]172[:]3219/LVLWPH[.]exe, hxxp[:]//192[.]210[.]239[.]172[:]3219/MCUCAT[.]exe,

TYPE	VALUE
URLs	hxxp[:]//192[.]210[.]239[.]172[:]3219/TJPLYT[.]exe, hxxp[:]//192[.]210[.]239[.]172[:]3219/z44[.]exe, hxxps[:]//cdn[.]lgaircon[.]xyz[:]443/jquery-3[.]3[.]1[.]min[.]js, hxxps[:]//192[.]210[.]239[.]172/messages/73KWf-o0-s0hxVCDJp1sfAHRcgdm7
File Path	C:\windows\temp\z1.exe, C:\windows\temp\z2.exe, C:\windows\temp\z44.exe, C:\windows\temp\z55.exe, C:\Windows\Temp\UDGEZR.exe, C:\Windows\Temp\z55.exe_winpty\winpty-agent.exe, C:\Windows\Temp\z55.exe_winpty\winpty.dll
IPv4:Port	192[.]210[.]239[.]172[:]3219, 192[.]210[.]239[.]172[:]4219, 192[.]210[.]239[.]172[:]2219

Patch Details

To address the CVE-2025-0994 vulnerability, which is actively being exploited in the wild, the patch should be applied by upgrading Trimble Cityworks to version 15.8.9 and Cityworks with Office Companion to version 23.10.

Reference Link:
https://learn.assetlifecycle.trimble.com/i/1532182-cityworks-customer-communication-2025-02-06-docx/0?

References

https://blog.talosintelligence.com/uat-6382-exploits-cityworks-vulnerability/

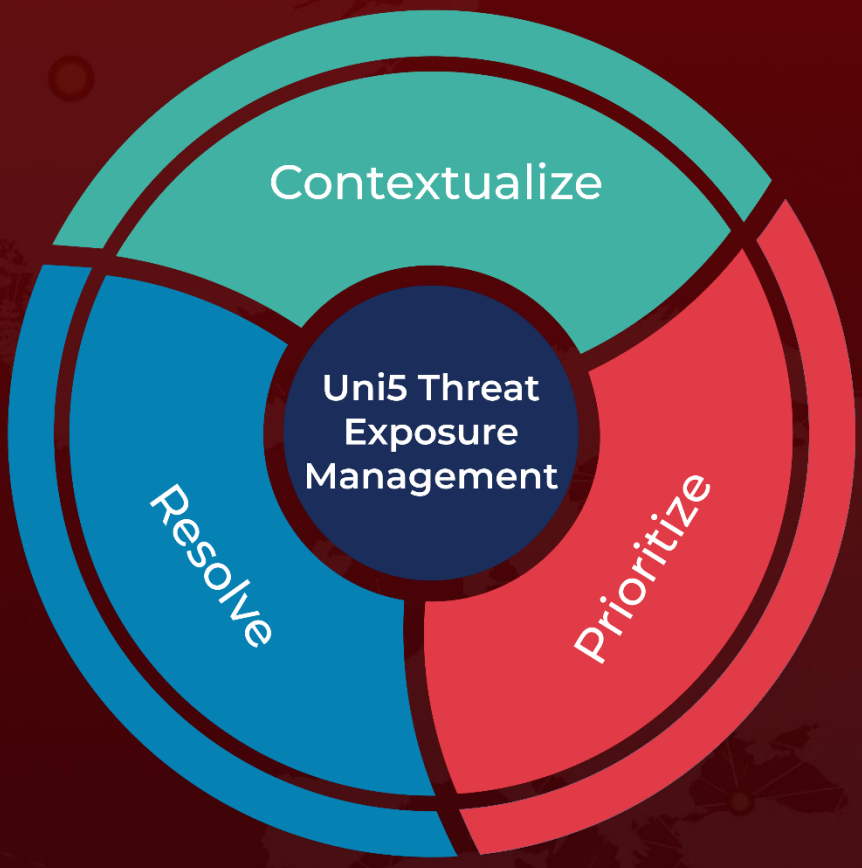
https://www.cisa.gov/news-events/ics-advisories/icsa-25-037-04

https://hivepro.com/threat-digest/cisa-known-exploited-vulnerability-catalog-february-2025/

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

May 23, 2025 • 6:30 AM

More at www.hivepro.com