TLP:CLEAR

Cyber Incidents Involving Cityworks Software

EPA is issuing this alert to inform water and wastewater system owners and operators of cyber incidents involving Cityworks Software. The Cityworks (Owned by Trimble) platform is used widely by State, Local, Tribal, and Territorial municipalities, including water and wastewater systems.

This alert encourages water and wastewater system/utility stakeholders to search for any indicators of system compromise (IOC) using the indicators and refer to the mitigations below for recommended steps to protect their systems.

Indicators of Compromise (IOC)

IOCs are digital evidence suggesting an Information Technology (IT)/Operational Technology (OT) system may have been breached. Below are known IOCs for this specific incident:

Indicator of Compromise	Type	Description
4b7561e27c87a1895446d7f2b83e2d9fcf71e6d6e8bc99d44818dc39a6ff99d5	SHA256 Hash	Obfuscated JavaScript (JS) payload in %TEMP% folder
4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9	SHA256 Hash	Custom Rust loader executable with Golang code loaded in memory; loads VShell
8a6c735f3608719ec9f46d9c6c5fc196db8c97065957c218b98733a491edd899	SHA256 Hash	Unknown
883d849b94238c26c57c0595ccb95b8c356628887b9a3628bf56e726332af925	SHA256 Hash	Custom Rust loader executable with Cobalt Strike loaded in memory

151a71c43e63db802d41d5d715aa98eb1b236e0a6441076a8d30fd93990416b4	SHA256 Hash	Unknown
1de72c03927bcd2810ce98205ff871ef1ebf4344fba187e126e50caa1e43250b	SHA256 Hash	Custom Rust loader executable with Cobalt Strike loaded in memory
14a072113baa0a1e1e2b6044068c7bc972ae5e541a0aec06577b0d6663140079	SHA256 Hash	Malicious File csidl_windows\temp\fq1u4t83.exe
04dc3a16e1e2b4924943805a1cea5e402c4f2304c717ea21fdf43274b8c34a84	SHA256 Hash	Malicious File csidl_windows\temp\q0pe6x96.exe
f09b51b759dfe7de06fa724bd89592f5b8eae57053d5fb4891e40f24055103fb	SHA256 Hash	Malicious File csidl_windows\temp\szm9wz8m.exe
C:\windows\temp\z1.exe	File Path	Malicious binary download path
C:\windows\temp\z2.exe	File Path	Malicious binary download path
C:\windows\temp\z44.exe	File Path	Malicious binary download path
C:\windows\temp\z55.exe	File Path	Malicious binary download path
C:\Windows\Temp\UDGEZR.exe	File Path	Malicious binary download path
C:\Windows\Temp\z55.exe_winpty\winpty-agent.exe	File Path	PUTTY binary download path
C:\Windows\Temp\z55.exe_winpty\winpty.dll	File Path	PUTTY binary download path
192.210.239[.]172:3219	IPv4:Port	Staging IP address
192.210.239[.]172:4219	IPv4:Port	Staging IP address
23.247.136[.]238	IPv4	Web application client address at the timestamp of malicious activity
31.59.70[.]13	IPv4	Web application client address at the timestamp of malicious activity

31.59.70[.]11	IPv4	Web application client address at the timestamp of malicious activity
149.112.117[.]49	IPv4	Web application client address at the timestamp of malicious activity
cdn.phototagx[.]com	Domain	Actor-controlled callback domain
https[:]//cdn.lgaircon[.]xyz[:]443/jquery-3.3.1.min.js	URI	Cobalt Strike C2
https[:]//192.210.239[.]172/messages/73KWf-o0-s0hx VCDJp1sfAHRcgdm7	URI	Cobalt Strike C2
192.210.137[.]81	IPv4	IP address likely controlled by the same threat actor
192.210.183[.]118	IPv4	IP address likely controlled by the same threat actor
ifode[.]xyz	Domain	Domain likely controlled by the same threat actor

Mitigation

All water and wastewater systems are recommended to:

1. Install the latest available patches/updates immediately. Trimble has released updated versions to both 15.x (15.8.9 published on January 28, 2025) and Cityworks 23.x software releases (23.10 published on January 29, 2025). Information on the updated versions is available through the Cityworks Support Portal.

   Please note: If you are unsure who hosts your Cityworks deployment or are hosted by a third party and do not have access to the customer portal, please contact your third-party hosting provider directly for additional information and assistance

2. Do not run Internet Information Services (IIS) with local or domain-level administrative privileges on any site.

3. Ensure that attachment directory root configurations are limited to folders/subfolders containing only attachments.

For additional information on mitigation techniques, please visit: CISA’s ICS Advisory – Trimble Cityworks.

Conclusion

For more information on the alert, please refer to CISA's ICS Advisory – Trimble Cityworks. Water and wastewater system owners and operators should direct their IT/OT system administrators to review this alert for further use and implementation. Organizations are encouraged to report suspicious or criminal activity information to the FBI Internet Crime Complaint Center (IC3) at IC3.gov or CISA via CISA's Incident Reporting System. If you have questions about any of the information contained in this document, please contact the Water3 Infrastructure and Cyber Resilience Division, Cybersecurity Branch at watercyberta@epa.gov.