

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical WhatsUp Gold Flaw POC Leads to Active Attacks

Date of Publication

September 19, 2024

Admiralty Code

A1

TA Number

TA2024363










Summary

First Seen: August 16, 2024

Affected Product: Progress WhatsUp Gold

Impact: Attackers are exploiting critical SQL injection vulnerabilities, including CVE-2024-6670, in WhatsUp Gold, targeting unpatched systems. Active exploitation has been observed since the publication of proof-of-concept (PoC) exploit code on August 30. Despite updates from August 16, many organizations remain vulnerable, with attackers using these flaws to deploy remote access tools and raising concerns about potential ransomware attacks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-6670	Progress WhatsUp Gold SQL Injection Vulnerability	Progress WhatsUp Gold			
CVE-2024-6671	Progress WhatsUp Gold SQL Injection Vulnerability	Progress WhatsUp Gold			
CVE-2024-6672	Progress WhatsUp Gold SQL Injection Vulnerability	Progress WhatsUp Gold			

Vulnerability Details

#1

Attackers have recently begun exploiting critical vulnerabilities in Progress Software's WhatsUp Gold network monitoring tool, specifically targeting organizations that have not yet applied the available security patches. These vulnerabilities, tracked as CVE-2024-6670, CVE-2024-6671, and CVE-2024-6672 are SQL injection flaws that allow attackers to retrieve encrypted passwords without authentication, making systems vulnerable to unauthorized access.

#2

Although Progress Software released updates to address these issues on August 16, many organizations have delayed implementing the fixes, leaving their networks exposed. Exploitation of these vulnerabilities has been observed since August 30, 2024, following the publication of proof-of-concept (PoC) exploit code by a security researcher.

#3

This PoC demonstrated how attackers could exploit improper input sanitization to bypass authentication, allowing arbitrary passwords to be inserted into administrator account fields and compromising those accounts. Within just five hours of the PoC release, active attacks were detected.

#4

Researchers have observed attackers using WhatsUp Gold's legitimate Active Monitor PowerShell Script functionality to deploy malicious PowerShell scripts via NmPoller.exe, downloaded from remote URLs. These scripts allow attackers to install various remote access tools (RATs), including Atera Agent, Radmin, SimpleHelp Remote Access, and Splashtop Remote, by leveraging the legitimate Windows utility 'msiexec.exe' to plant these tools.

#5

By deploying these RATs, attackers can establish persistence on compromised systems, maintaining long-term access for further malicious activities. The exploitation frequently involves multiple payloads, suggesting potential involvement of ransomware actors, although no specific threat groups have been identified. Notably, this is not the first incident involving WhatsUp Gold, as a similar vulnerability (CVE-2024-4885) was exploited earlier this year.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-6670	Progress WhatsUp Gold versions released before 2024.0.0	cpe:2.3:a:progress:what sup_gold:*.:*.*.*.*.*.*	CWE-89
CVE-2024-6671	Progress WhatsUp Gold versions released before 2024.0.0	cpe:2.3:a:progress:what sup_gold:*.:*.*.*.*.*.*	CWE-89
CVE-2024-6672	Progress WhatsUp Gold versions released before 2024.0.0	cpe:2.3:a:progress:what sup_gold:*.:*.*.*.*.*.*	CWE-89

Recommendations



Apply Patches and Updates: Ensure that your systems running WhatsUp Gold are updated with the latest patches provided by Progress. Keeping software up to date is critical to protect against known exploits.



Network Segmentation and Least Privilege: Segment critical systems and restrict network access to them. Implementing the principle of least privilege ensures that even if an attacker gains access through this vulnerability, their ability to move laterally within your network will be limited. This reduces the overall damage potential.



Monitor for Suspicious Activity: Continuously monitor process creation events, especially those related to NmPoller.exe or PowerShell script execution. Suspicious scripts or downloads, such as those initiating from external URLs, should trigger alerts for further investigation.



Implement Strong Authentication: Strengthen authentication mechanisms, including the use of multi-factor authentication (MFA) and strong, unique passwords. Avoid using default or weak credentials, as attackers can exploit these even if patches are applied



Potential MITRE ATT&CK TTPs

<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0005</u> Defense Evasion
<u>TA0003</u> Persistence	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1203</u> Exploitation for Client Execution	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.001</u> PowerShell	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1218.007</u> Msixexec	<u>T1218</u> System Binary Proxy Execution		

Indicator of Compromise (IOCs)

TYPE	VALUE
File Path	C[:]ProgramData\a[.]ps1, C[:]windows\temp\MSsetup[.]msi, C[:]ProgramData\ftpd32[.]exe
SHA256	6daa94a36c8ccb9442f40c81a18b8501aa360559865f211d72a74788a1bbf3ce, f1c68574167eaea826a90595710e7ee1a1e75c95433883ce569a144f116e2bf4, 992974377793c2479065358b358bb3788078970dacc7c50b495061ccc4507b90
IPv4	185[.]123[.]100[.]160
URLs	hxxps[:]//webhook[.]site/b6ef7410-9ec8-44f7-8cdf-7890c1cf5837, hxxps[:]//fedko[.]org/wp-includes/ID3/setup[.]msi, hxxp[:]//45[.]227[.]255[.]216[:]29742/ddQCz2CkW8/setup[.]msi, hxxp[:]//185[.]123[.]100[.]160/access/Remote Access-windows64-offline[.]exe

Patch Details

Upgrading to WhatsUp Gold 2024.0.0, direct upgrades are supported from WhatsUp Gold version 20.0.2 and newer.

Link:

<https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-August-2024>

References

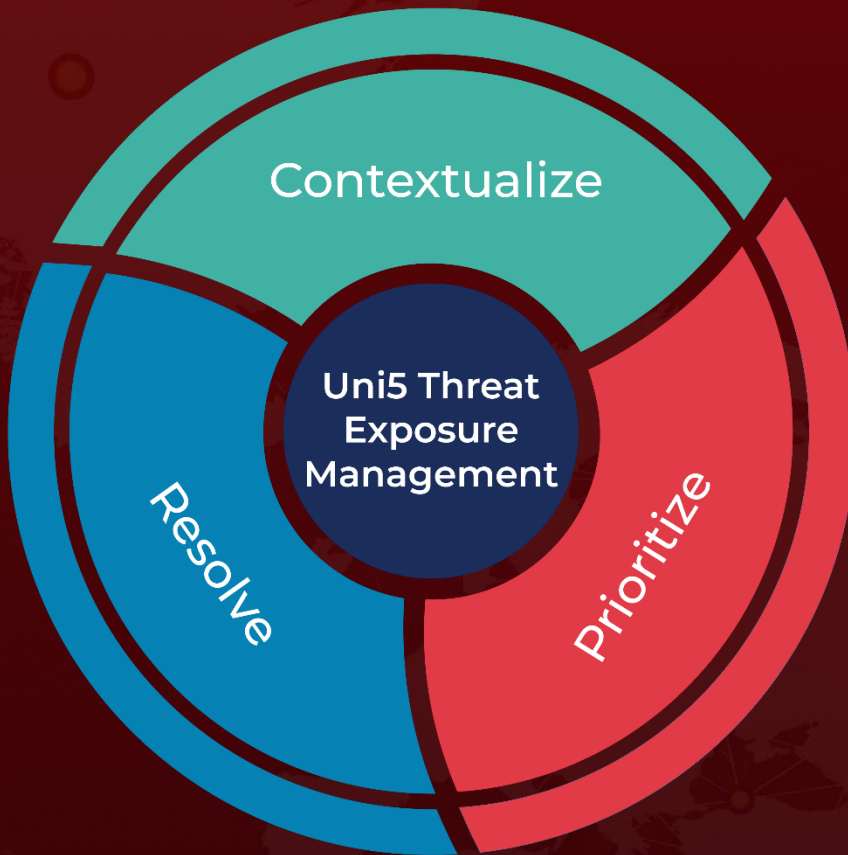
https://www.trendmicro.com/en_us/research/24/i/whatsup-gold-rce.html

<https://summoning.team/blog/progress-whatsup-gold-sqli-cve-2024-6670/>

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

September 19, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com