

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Vulnerabilities Patched in Progress Software's MOVEit

Date of Publication

June 27, 2024

Admiralty Code

A1

TA Number

TA2024247







Summary

First Seen: June 25, 2024

Affected Product: Progress MOVEit Transfer, Progress MOVEit Gateway

Impact: Progress Software fixed critical vulnerabilities CVE-2024-5805 (in MOVEit Gateway) and CVE-2024-5806 (in MOVEit Transfer), addressing authentication bypass issues in SFTP modules. Patches require system downtime for installation and are available for both on-premises and MOVEit Cloud deployments, urging immediate updates to mitigate risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-5806	Progress MOVEit Transfer Improper Authentication Vulnerability	Progress MOVEit Transfer			
CVE-2024-5805	Progress MOVEit Gateway Improper Authentication Vulnerability	Progress MOVEit Gateway			

Vulnerability Details

#1

Progress Software recently addressed two significant vulnerabilities in its MOVEit managed file transfer software. The first, CVE-2024-5805, affects MOVEit Gateway v2024.0.0 and allows attackers to bypass authentication in the SFTP module. This critical flaw was patched in v2024.0.1, requiring system downtime during the upgrade.

#2

The second vulnerability, CVE-2024-5806, impacts various versions of MOVEit Transfer, enabling authentication bypass under specific conditions within the SFTP module. It has been fixed in the latest software versions for both on-premises and cloud deployments.

#3

Security researchers have detailed in a Proof-of-Concept of CVE-2024-5806, that it could be exploited to impersonate any user on the server, posing significant risks. The vulnerability involves two separate issues, one specific to Progress MOVEit and another affecting the IPWorks SSH library.

#4

As of recent data, around 2,700 MOVEit Transfer instances are online globally, primarily in several countries including the U.S., U.K., Germany, and others. The urgency to update to the latest software versions is underscored by [previous instances of exploitation](#), highlighting the critical need for mitigation measures against such vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-5806	Progress MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2	cpe:2.3:a:progress: moveit_transfer:*:* :*:*:*:*:*	CWE-287
CVE-2024-5805	MOVEit Gateway 2024.0.0	cpe:2.3:a:progress: moveit_gateway:*:* :*:*:*:*:*	CWE-287

Recommendations



Apply Vendor Patches Immediately: Ensure all affected versions of MOVEit Transfer and MOVEit Gateway are updated to the latest patched versions provided by Progress Software. These patches address the authentication bypass vulnerabilities and should be applied promptly.



Implement Network Security Measures: Block public inbound RDP access to MOVEit Transfer servers to minimize exposure to external threats. Limit outbound access from MOVEit Transfer servers to only known and trusted endpoints. This reduces the risk of unauthorized data exfiltration or further compromise.



Monitor and Audit System Activity: Implement logging and monitoring mechanisms to detect any unusual or unauthorized access attempts or system activities related to SFTP services. Regularly review logs for signs of exploitation attempts.



Best Practices: Follow general security best practices, such as keeping software and firmware up to date, using strong authentication mechanisms, and employing endpoint protection solutions.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0001</u> Initial Access	<u>TA0004</u> Privilege Escalation
<u>T1078</u> Valid Accounts	<u>T1190</u> Exploit Public-Facing Application	<u>T1588.005</u> Exploits	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities		

Patch Links

<https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806>

<https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805>

References

<https://labs.watchtowr.com/auth-bypass-in-un-limited-scenarios-progress-moveit-transfer-cve-2024-5806/>

<https://x.com/Shadowserver/status/1805676078620401831>

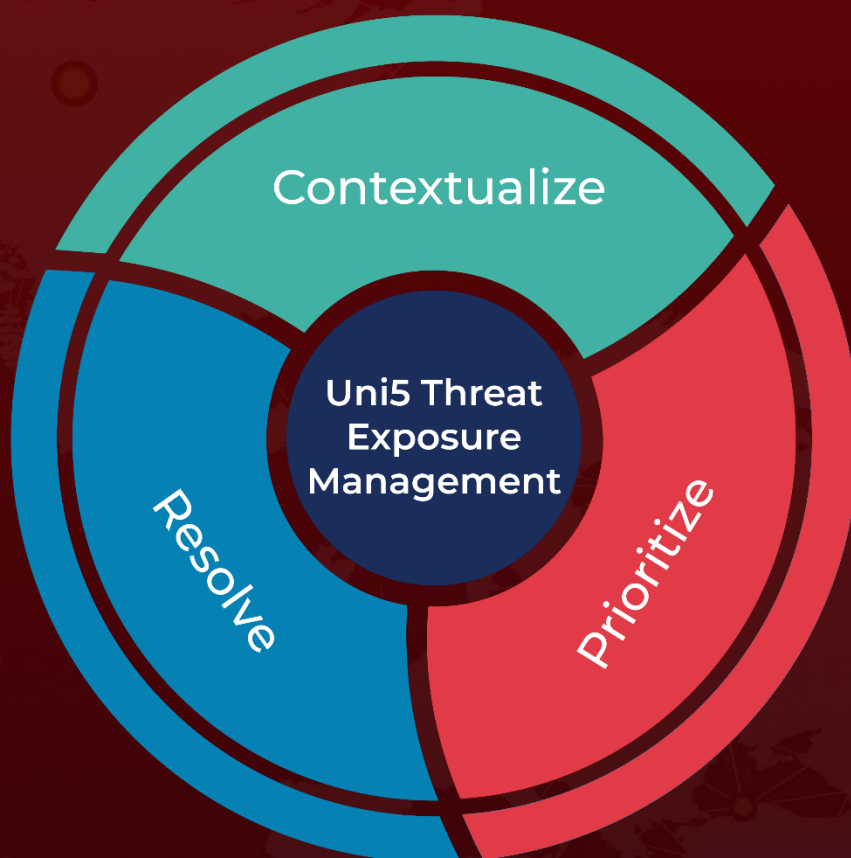
<https://censys.com/moveit-transfer-auth-bypass/>

<https://www.hivepro.com/the-exploitation-of-critical-zero-day-vulnerability-found-in-moveit-transfer/>

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

June 27, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com