

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Atera Addressed Two Zero-Day Vulnerabilities Exploiting MSI Files

Date of Publication

July 25, 2023

Admiralty Code

A1

TA Number

TA2023312







Summary

First Seen: February 28, 2023

Affected Platforms: Atera Agent Windows

Impact: The privilege escalation vulnerabilities in MSI installers, enable attackers to elevate privileges, potentially leading to full system control and unauthorized access. Timely patches and secure configuration are essential to prevent these impactful attacks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-26077	Atera Agent Windows Privilege Escalation	Atera Agent Windows			
CVE-2023-26078	Atera Agent Windows Privilege Escalation	Atera Agent Windows			

Vulnerability Details

#1

Windows Installers for the Atera remote monitoring and management software contain two zero-day vulnerabilities that could serve as a starting point for launching privilege escalation attacks. The first vulnerability (CVE-2023-26077) was identified in the MSI installer for Atera Agent version 1.8.3.6. It involved misconfigured Custom Actions running as NT AUTHORITY\SYSTEM during the repair functionality. Attackers could exploit this flaw to execute a local privilege escalation attack through DLL hijacking. By dropping a malicious payload into a specific folder with improper permissions, they could gain NT AUTHORITY\SYSTEM privileges and execute arbitrary code.

#2

Another vulnerability (CVE-2023-26078) found in Atera's Windows installer was the execution of system commands that triggered the Windows Console Host (conhost.exe) as a child process. This could briefly open a command window, which attackers could exploit for local privilege escalation. By manipulating the command window, they could access hyperlinks to open a web browser as NT AUTHORITY\SYSTEM and further escalate privileges.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-26077	Atera Agent versions 1.8.3.6 and before	cpe:2.3:a:atera:agent:1.8.3.x:*:*:*:*:*	CWE-379
CVE-2023-26078	Atera Agent versions 1.8.4.8 and before	cpe:2.3:a:atera:agent:1.8.4.x:*:*:*:*:*	CWE-648

Recommendations



Regularly Patch and Update: Keep systems and software up-to-date with the latest patches and updates from vendors. CVEs were addressed through software fixes, which is a crucial step in mitigating known vulnerabilities. Timely updates ensure that potential security risks are minimized and that newly discovered vulnerabilities are patched promptly.



Secure Custom Actions: Software developers should thoroughly review and secure Custom Actions in MSI files to prevent potential privilege escalation attacks. Misconfigured Custom Actions can lead to serious security risks. It is essential to restrict and properly manage the permissions of actions executed with NT AUTHORITY\SYSTEM privileges to ensure only authorized operations can be performed.



Monitor and Analyze Event Logs: Continuously monitor event logs, particularly Application event ID 11728, to detect and respond to potential MSI repair privilege escalation attacks. This event ID is specifically associated with MSI repairs and can provide valuable information, such as the affected product, the user involved, and the date of the event.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1203</u> Exploitation for Client Execution	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.001</u> PowerShell
<u>T1574.001</u> DLL Search Order Hijacking	<u>T1574</u> Hijack Execution Flow		

Patch Details

CVE-2023-26077: The vulnerability fixed in ATERA AGENT version 1.8.3.7

CVE-2023-26078: The vulnerability fixed in ATERA AGENT version 1.8.4.9

References

<https://www.mandiant.com/resources/blog/privileges-third-party-windows-installers>

<https://github.com/mandiant/Vulnerability-Disclosures/commit/79876c537b1ca3a766a50b9f2c518cf8aed860ea>

<https://socradar.io/zero-days-cve-2023-26077-cve-2023-26078-in-atera-windows-installers/>

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

July 25, 2023 • 6:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com