Lazarus Group Exploits ManageEngine Vulnerability

Executive Summary
Cisco Talos has published an open-source report regarding the North Korean state-sponsored actor, the Lazarus Group, reported to be targeting internet backbone infrastructure and healthcare entities in Europe and the United States. The attackers have been exploiting a vulnerability in ManageEngine products, which is tracked as CVE-2022-47966. This vulnerability was added to CISA’s Known Exploited Vulnerabilities Catalog in January 2023. Through this exploit, the attackers are deploying the remote access trojan (RAT) known as “QuiteRAT.” Security researchers previously identified this malware in February 2023, and it is reportedly the successor to the group’s previously used malware “MagicRAT,” which contains many of the same capabilities. Further analysis of this campaign has also shown that the group is using a new malware tool called “CollectionRAT,” which appears to operate like most RATs by allowing the attacker to run arbitrary commands among other capabilities. Both CISA and the FBI have previously warned that these types of vulnerabilities are common attack methods for malicious actors and can pose a significant risk to healthcare and public health organizations. HC3 strongly encourages organizations to update these systems.

Report
CVE-2022-47966 is a critical vulnerability that affects twenty-four of ManageEngine’s products and allows an attacker to perform remote code execution. This vulnerability is exploitable if the SAML single-sign-on is or ever has been enabled in the ManageEngine setup. Approximately five days after the proof-of-concept for this vulnerability appeared online, North Korean actors began exploiting it. Through this vulnerability, the state sponsored group Lazarus has reportedly been targeting internet backbone infrastructure and healthcare entities in Europe and the United States.

After gaining initial access through this vulnerability, the group has been deploying the remote access trojan, QuiteRAT. QuiteRAT is believed to be the successor of the group’s previously-used malware MagicRAT, and it contains many of the same capabilities, such as arbitrary command execution. Both implants are built on the Qt framework. Use of the Qt framework makes human analysis more difficult when compared to other programming languages. The use of Qt is not regularly used in malware development, which makes machine learning and heuristic analysis of it being less reliable. Additionally, QuiteRAT also has a significantly smaller file size, going from 18MB to 4MB while still retaining its original functionality. One of the reasons for the smaller file size is that QuiteRAT lacks the ability to perform persistence capabilities on its own, and the hackers must accomplish this task separately.

The Lazarus Group was observed using the cURL command to deploy the QuiteRAT binary:

According to Cisco Talos, “…a successful download of the binary leads to the execution of the QuiteRAT
binary by the Java process, resulting in the activation of the implant on the infected server. Once the implant starts running, it sends out preliminary system information to its command and control (C2) servers, and then waits on the C2 to respond with either a command code to execute or an actual Windows command to execute on the endpoint via a child cmd.exe process. Some of the initial commands executed by QuiteRAT on the endpoint are for reconnaissance.”

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>`C:\windows\system32\cmd.exe /c systeminfo</td>
<td>findstr Logon`</td>
</tr>
<tr>
<td>`C:\windows\system32\cmd.exe /c ipconfig</td>
<td>findstr Suffix`</td>
</tr>
</tbody>
</table>

In addition to the use of QuiteRAT, Lazarus is using a new malware called “CollectionRAT.” Researchers have noted that CollectionRAT appears to have standard RAT capabilities, such as running arbitrary commands on the compromised system. This new threat is believed to be connected to the Jupiter/EarlyRAT malware family, which has previously been linked to a Lazarus subgroup, Andariel. CollectionRAT is also used for gathering metadata, managing files on the infected system, and delivering additional payloads.
Indicators of Compromise
The following links contain available indicators of compromise (IOCs) that organizations can use to identify any possible IOCs in their ManageEngine products:

ManageEngine CVE-2022-47966 IOCs:

Cisco Talos IOCs:
https://github.com/Cisco-Talos/IOCs/tree/main/2023/08

<table>
<thead>
<tr>
<th>Cisco Talos QuiteRAT IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ed8ec7a8dd089019cfdd9143f008fa0951c56a35d73b2e1b274315152d0c0ee6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco Talos CollectionRAT IOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eeed9338984</td>
</tr>
<tr>
<td>773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df</td>
</tr>
</tbody>
</table>

Patches, Mitigations, and Workarounds
According to the vendor's security advisory, CVE-2022-47966 allows for unauthenticated remote code...
execution in twenty-four of the ManageEngine products. This issue can be fixed by updating the third party module to the most recent version, and HC3 strongly encourages applying this update as soon as possible to avoid any potential compromise.

References


Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback