Ransomware Attackers May Have Used Privilege Escalation Vulnerability as Zero-day

symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day

Threat Hunter TeamSymantec

Some evidence to suggest that attackers linked to Black Basta compiled CVE-2024-26169 exploit prior to patching.

The Cardinal cybercrime group (aka Storm-1811, UNC4393), which operates the Black Basta ransomware, may have been exploiting a recently patched Windows privilege escalation vulnerability as a zero-day.

The vulnerability (CVE-2024-26169) occurs in the Windows Error Reporting Service. If exploited on affected systems, it can permit an attacker to elevate their privileges. The vulnerability was patched on March 12, 2024, and, at the time, Microsoft said there was no

evidence of its exploitation in the wild. However, analysis of an exploit tool deployed in recent attacks revealed evidence that it could have been compiled prior to patching, meaning at least one group may have been exploiting the vulnerability as a zero-day.

Black Basta link

The exploit tool was deployed in a recent attempted ransomware attack investigated by Symantec's Threat Hunter Team. Although the attackers did not succeed in deploying a ransomware payload in this attack, the tactics, techniques, and procedures (TTPs) used were highly similar to those described in a recent Microsoft report detailing Black Basta activity. These included the use of batch scripts masquerading as software updates.

Although no payload was deployed, the similarities in TTPs makes it highly likely it was a failed Black Basta attack.

Exploit tool

Analysis of the exploit tool revealed that it takes advantage of the fact that the Windows file werkernel.sys uses a null security descriptor when creating registry keys. Because the parent key has a "Creator Owner" access control entry (ACE) for subkeys, all subkeys will be owned by users of the current process. The exploit takes advantage of this to create a "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WerFault.exe" registry key where it sets the "Debugger" value as its own executable pathname. This allows the exploit to start a shell with administrative privileges.

The variant of the tool used in this attack (SHA256: 4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63) had a compilation time stamp of February 27, 2024, several weeks before the vulnerability was patched.

A second variant of the tool discovered on Virus Total (SHA256: b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0) had an earlier compilation time stamp of December 18, 2023.

Time stamp values in portable executables are modifiable, which means that a time stamp is not conclusive evidence that the attackers were using the exploit as a zero-day. However, in this case there appears to be little motivation for the attackers to change the time stamp to an earlier date.

Revived threat

Cardinal introduced Black Basta in April 2022 and from its inception, the ransomware was closely associated with the Qakbot botnet, which appeared to be its primary infection vector.

Qakbot was one of the world's most prolific malware distribution botnets until it was taken down following law enforcement action in August 2023. However, while the takedown led to a dip in Black Basta activity, Cardinal has since resumed attacks and now appears to have switched to working with the operators of the DarkGate loader to obtain access to potential victims.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63 – Exploit tool

b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0 – Exploit tool

a31e075bd5a2652917f91714fea4d272816c028d7734b36c84899cd583181b3d – Batch script

3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d – Batch script

2408be22f6184cdccec7a34e2e79711ff4957e42f1ed7b7ad63f914d37dba625 – Batch script

b0903921e666ca3ffd45100a38c11d7e5c53ab38646715eafc6d1851ad41b92e – ScreenConnect

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?