Windows SMB Zero Day Exploit Advisory

What happened?

US-CERT released a warning on Thursday 2/2/2017 about a Microsoft Windows vulnerability caused by a memory corruption bug in the handling of SMB traffic. This vulnerability may allow a remote, unauthenticated attacker to cause a denial of service (crash or reboot) on a vulnerable system.

The zero day has been confirmed to affect Windows clients that support SMBv3. This includes the following fully patched systems:

- Windows 10
- Windows 8.1
- Windows Server 2016
- Windows Server 2012R2
- http://www.kb.cert.org/vuls/id/867968

What is the issue?

The proof of concept code for exploiting the code has been released on the Internet and is publicly available. There are a number of ways an attacker could get a Windows device to connect to a malicious SMB share such as clicking on a URL link. A Windows device that connects to the malicious SMB share would either reboot or crash (Blue Screen of Death) causing a denial of service.

There is currently no patch available, hopefully one will be released on patch Tuesday.

Should we be concerned?

Yes, given that the vulnerability is fairly simple to exploit and the proof of concept is publically available companies should make sure they have taken steps to mitigate a potential denial of service to Windows systems.

What types of systems are vulnerable? [1]

Please refer to US-CERT Vulnerability Note VU#867968 for specific details.

hxxp://www.kb.cert.org/vuls/id/867968

For more Information on this zero day:

Reference US-CERT has guidance:

02/02/2017 (updated) CVE-2017-0016 Severity = MEDIUM

- hxxp:// www.kb.cert.org/vuls/id/867968

[1] Please replace hxxp:// references with http://

Additional References

- hxxp://github.com/lgandx/PoC/tree/master/SMBv3%20Tree%20Connect
- hxxp://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices
- hxxp://msdn.microsoft.com/en-us/library/cc246499.aspx

Recommended Actions

1. Block outbound SMB connections to the WAN (TCP ports 139 & 445 along with UDP ports 137 & 138).
2. Patch vulnerable Windows devices as soon as a patch is available.