CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-014

Critical Vulnerabilities in Microsoft NTLM

June 13, 2019 — v1.0

TLP:WHITE

History:

- *13/06/2019 — v1.0: Initial publication*

Summary

Two critical Microsoft vulnerabilities were discovered by the research team Preempt [1]. The vulnerabilities consist of three logical flaws in NTLM (NT Lan Manager). The vulnerabilities allow an attacker to potentially execute malicious code remotely or authenticate to any HTTP server that supports Windows Integrated Authentication (WIA) such as Exchange or ADFS.

Technical Details

The NTLM-relay attack has been out in the wild for some time. In short, it allows lateral movement in the target's network. Over the years, Microsoft has built defensive features to mitigate such an attack. However, in a proof of concept, the researchers from Preempt managed to bypass successfully the following mechanisms:

- Message Integrity Code (MIC)
- SMB Session Signing
- Enhanced Protection for Authentication (EPA, more details [4])

Microsoft has released two patches for CVE-2019-1040 [2] and CVE-2019-1019 [3] to address the issue, but a proper configuration is also required to be fully protected.

Products Affected

- All versions of Windows are affected.

Recommendations

- Apply patches to the workstations and servers.

Additionally, ensure a secure configuration by:

- Enforce SMB Signing
- Block NTLMv1
- Enforce LDAP/S Signing
- Enforce Enhanced Protection for Authentication
- Reduce NTLM usage

References

[1] https://blog.preempt.com/security-advisory-critical-vulnerabilities-in-ntlm

[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1040

[3] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1019

[4] https://blog.preempt.com/how-to-easily-bypass-epa