



PetitPotam NTLM Relay Attack

CRITICALITY 

11/08/2021

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A critical vulnerability that affects the Domain Controller via PetitPotam method is under active attack, and Microsoft recommends all the customers to install the latest update immediately.



Threat Details

On the 10th of August, Microsoft has released an update to plug a critical vulnerability tracked as CVE-2021-36942 impacting Domain Controller. The vulnerability uses Encrypting File System Remote Protocol (MS-EFSRPC) API functions (OpenEncryptedFileRawA and OpenEncryptedFileRawW) to force the domain controller to authenticate the threat actor's NTLM relay server. After that, The NTLM will try to gain Kerberos ticket-granting ticket (TGT) by sending a request to the Active Directory Certificate Services for the targeted system via HTTP.

In the latest update, Microsoft has blocked the affected API calls to OpenEncryptedFileRawA and OpenEncryptedFileRawW from the LSARPC interface. However, the company warns that applying the update may impact the backup software that utilizes the EFS API OpenEncryptedFileRawA and OpenEncryptedFileRawW functions.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks

References

Microsoft Releases Windows Updates to Patch Actively Exploited Vulnerability. (2021). Retrieved from The Hacker News: <https://thehackernews.com/2021/08/microsoft-releases-windows-updates-to.html>

Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS). (2021). Retrieved from Microsoft: <https://msrc.microsoft.com/update-guide/vulnerability/ADV210003>

Windows security update blocks PetitPotam NTLM relay attacks. (2021). Retrieved from BleepingComputer: <https://www.bleepingcomputer.com/news/microsoft/windows-security-update-blocks-petitpotam-ntlm-relay-attacks/>



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to patch **CVE-2021-36942** on the following affected products by installing the latest update:

- Windows Server 2012 (Server Core)
- Windows Server 2012 (Server Core)
- Windows Server 2012
- Windows Server 2012 (Server Core)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core)
- Windows Server 2008 R2 for x64-based Systems Service Pack1
- Windows Server 2008 R2 for x64-based Systems Service Pack1 (Server core)
- Windows Server 2008 R2 for x64-based Systems Service Pack2
- Windows Server 2008 R2 for x64-based Systems Service Pack2 (Server core)
- Windows Server 2008 R2 for x32-based Systems Service Pack2
- Windows Server 2008 R2 for x32-based Systems Service Pack2 (Server core)
- Windows Server 2016
- Windows Server 2016 (Server Core)
- Windows Server 2019
- Windows Server 2019 (Server Core)



Appendix B – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)



CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
- Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
- MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.