



High Severity MSDT Zero-Day Vulnerability in Microsoft

CRITICALITY 

01/06/2022

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

Microsoft released guidance for a recently disclosed zero-day vulnerability in MSDT that affects several versions of Microsoft Office. The company recommends all the customers follow the published workarounds as a temporary solution.



Threat Details

Microsoft released workarounds in its guidance for a newly discovered zero-day vulnerability in Microsoft Support Diagnostic Tool (MSDT) that impacts several versions of Microsoft Office. The addressed vulnerability was tracked as CVE-2022-30190 and known as "Follina" with a CVSS score of 7.8. It is a Remote Code Execution (RCE) vulnerability that can be exploited by an attacker sending a URL to a vulnerable machine. Successful exploitation allows an attacker to download arbitrary remote code and run it on a system with the privileges of the calling application. Moreover, an attacker can install programs, view, or modify data, or create new accounts in line with the victim's user permissions.

According to the published report, the Proof of Concept (PoC) code for exploitation is available online and has been integrated into common exploitation frameworks and tools. Unfortunately, disabling Microsoft Office Macros does not prevent the exploitation of this vulnerability.

MSDT flaw impact Microsoft Office versions 2013, 2016, 2019, and 2021, as well as Microsoft office 365. The company highly advises all customers to follow the published workarounds as a temporary solution.



Recommendations



Prevention

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



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

MRC. (2022, May 30). *Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability*. Retrieved from Microsoft Security Response Center: <https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/>

syloktools. (2022, May 31). *msdt-0-day.md*. Retrieved from GitHub: <https://github.com/NVISOsecurity/nviso-cti/blob/master/advisories/29052022%20-%20msdt-0-day.md>



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 the following steps:

- Disabling MSDT URL protocol:
 - Run Command Prompt as Administrator.
 - To back up the registry key, execute the command:
"reg export HKEY_CLASSES_ROOT\ms-msdt filename "
 - Execute the command: *"reg delete HKEY_CLASSES_ROOT\ms-msdt /f"*
- To undo the workaround:
 - Run Command Prompt as Administrator.
 - To restore the registry key, execute the command: *"reg import filename"*
- Block all Office applications from creating child processes by enabling the following rule in d PowerShell prompt:
Set-MpPreference -AttackSurfaceReductionRules_Iids d4f940ab-401b-4efc-aadc-ad5f3c50688a -AttackSurfaceReductionRules_Actions Enabled

Affected Products:

- Microsoft Office version 2013
- Microsoft Office version 2016
- Microsoft Office version 2019
- Microsoft Office version 2021
- Microsoft Office 365



Appendix B – Detection

Detections:

- Microsoft Defender Antivirus detections:
 - Trojan:Win32/Mesdetty.A (blocks msdt command line)
 - Trojan:Win32/Mesdetty.B (blocks msdt command line)
 - Behavior:Win32/MesdettyLaunch.A!blk (terminates the process that launched msdt command line)
- Microsoft Defender for Endpoint customers detections:
 - Suspicious behavior by an Office application
 - Suspicious behavior by Msdt.exe
- Keep an eye on child processes with the sdiagnhost.exe parent process.

Indicators of Compromise

Type	Value
Domains	http://coolrat[.]xyz hxxps[:]//www[.]xmlformats[.]com/office/word/2022/wordprocessingDrawing/RDF842I[.]html!
Hashes	4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784



Appendix C – 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.