Vulnerability Alert

Alert No : AVA171020

Date : 20-Oct-17 17:18 PM

Microsoft Word Exploited!

Overview	Recently discovered unpatched Microsoft Word DDE Exploit is currently being used in a widespread malware attack campaigns. (This is not a macro based malware)
Description / Impact	• **The DDE vulnerability is a macro-less code execution malware.** • **A security warning isn't displayed to the user when the word document is opened. But requests the user if he/she wants to execute the application specified in the command.** • **The newly discovered DDE technique is currently in use by the attackers to deliver malware via email around the world using Necurs Botnet and have the ability to take screenshots of the desktops of the victims.** • **Hanictor Malware (also known as Chanitor and Tordal) uses the Microsoft Office DDE exploit. This malware is a downloader that has the capability to install malicious payloads like Banking Trojans and Ransomware which is delivered as a macro-enabled MS office document in phishing emails.**
Risk Reduction Recommendations	**Immediate Actions to be taken:** 1. Disable the 'update automatic links at open' option in the MS Office programs. • *Open Word → Select File → Options → Advanced and scroll down to General and then uncheck "Update Automatic links at Open."* 2. Always be suspicious on unsolicited email attachments. 3. It is highly advisable to inform the staff to be vigilant.
Reference	https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
Disclaimer	**The information provided herein is on "as is" basis, without warranty of any kind.**

Financial Sector Computer Security Incident Response Team, Sri Lanka
Hotline: + 94 112039777
Report incident to incident@fincsirt.lk