Avviso di sicurezza del 08/07/2022

# Segnalazione di una vulnerabilità 0-day Follina presente in Microsoft Word

Gentili Utenti,
pubblichiamo questo avviso per segnalare la presenza di una vulnerabilità 0-day che affligge l'applicativo Microsoft Word attivamente sfruttata in questi giorni. Tale vulnerabilità permette di eseguire codice arbitrario attraverso l'apertura di un documento Word opportunamente forgiato. Allo stato del presente avviso non sono disponibili correttivi; occorre quindi prestare la massima prudenza nell'apertura di documenti di tipo Microsoft Word non richiesti. Nel caso di ricezione di un tale documento, si consiglia di richiedere all'interlocutore mittente la verifica dell'autenticità dell'inviO. Nel caso non sia possibile verificare l'affidabilità del documento potete inoltrare le mail sospette a sicurezza@unimi.it per un controllo ulteriore. Di seguito sono riportati maggiori dettagli su questa vulnerabilità.

Grazie per l'attenzione.

I più cordiali saluti.

Settore Cybersecurity, Protezione Dati e Conformita' - Direzione ICT
Universita' degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

---
UNIMI-SOC-202206080000000002 Per favore, usate questa riga per le comunicazioni su questa segnalazione

## Dettagli della vulnerabilità

La maggior parte dei virus veicolati tramite Microsoft Office si basa sull'uso di macro; è possibile proteggersi da tali attacchi disabilitando l'esecuzione delle macro ed avendo una certa prudenza nell'apertura di documenti Office di dubbia provenienza. La vulnerabilità scoperta in questi giorni, chiamata Follina si basa su un meccanismo differente che, purtroppo, non richiede nessuna interazione con l'utente: è sufficiente aprire un file di testo tramite Microsoft Word per eseguire uno script pericoloso.

Il funzionamento di tale vulnerabilità in un possibile attacco è il seguente:

- L'utente apre un file di testo con estensione ".doc", ricevuto, ad esempio, via mail.
- All'apertura del documento, Microsoft Word viene indotto a scaricare un contenuto malevolo via web in formato HTML
- Il documento malevolo HTML provoca l'attivazione del Microsoft Support Diagnostic Tool (msdt.exe) che a sua volta esegue codice malevolo PowerShell

Maggiori informazioni sono reperibili al link di seguito:

https://www.linkedin.com/pulse/follina-new-vulnerability-microsoft-office-axence-net?trk=pulse-article_more-articles_related-content-card

Allo stato del presente avviso non è ancora disponibile una patch risolutiva. Nel caso si stia usando un sistema con sistema operativo Windows occorre quindi prestare attenzione nell'apertura di documenti specie se arrivati via posta elettronica. Nel caso di documenti Word prima dell'apertura è indispensabile accertarsi della genuinità del documento chiedendo conferma al mittente attraverso un metodo affidabile (chiamata telefonica, verifica con i colleghi). Nel caso non sia possibile verificare l'affidabilità del documento potete inoltrare le mail sospette a sicurezza@unimi.it per un controllo ulteriore.