02/04/2021

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 674
Utenti unici: 1.633

https://www.cybersecurity360.it/nuove-minacce/microsoft-exchange-analisi-dellattacco-ecco-perche-le-patch-potrebbero-non-bastare/

Microsoft Exchange, analisi dell'attacco: ecco perché le patch potrebbero non bastare

L'analisi dell'attacco contro i server Microsoft Exchange condotto mediante lo sfruttamento di alcune vulnerabilità note (e ora risolte), consente di comprendere le tecniche utilizzate dai cyber criminali in modo da adottare le necessarie contromisure. Anche perché le singole patch potrebbero non bastare Negli Stati Uniti è stata recentemente sfruttata da un gruppo di cracker la vulnerabilità CVE-2021-26855 per condurre un attacco di tipo Server-Side Request Forgery verso i server Microsoft Exchange.Sfruttando questa vulnerabilità i cyber criminali possono accedere ai servizi di posta elettronica, attraverso richieste HTTP, causando perdita di informazioni anche sensibili oppure caricare altro malware sulla macchina target.Gli attaccanti, tramite questa catena di attacchi, sono riusciti ad accedere a diversi account riuscendo a leggere un gran numero di e-mail degli utenti, molte contenenti anche informazioni sensibili.Ovviamente, attraverso queste e-mail rubate è stato possibile eseguire attacchi di tipo phishing verso altri utenti all'interno della rete.Inoltre, possiamo ipotizzare che l'intento degli attaccanti fosse quello di un Advanced Persistent Threat (APT), cioè un attacco mirato e persistente portato avanti grazie a un notevole expertise tecnico e grandi risorse anche economiche.Indice degli argomenti I passaggi dell'attacco ai server Microsoft ExchangeSoluzioni per mitigare il rischio di un attacco a Exchange Ecco perché aggiornare i sistemi potrebbe non bastare I passaggi dell'attacco ai server Microsoft Exchange Sebbene l'attacco inizi con l'autenticazione ai sistemi compromessi tramite la vulnerabilità CVE-2021-26855, gli attaccanti potrebbero accedere ai sistemi per altre vie sfruttando altre vulnerabilità, ad esempio password deboli. WEBINAR WEBINAR - Garantire la sicurezza dei dati nell'era della collaboration online Sicurezza Software Iscriviti al WebinarOvviamente, come per ogni vulnerabilità, il cyber criminale ha bisogno di accedere ad un'istanza del server attraverso la porta 443. Successivamente, l'attaccante può iniziare a procedere all'ottenimento del controllo di questi dispositivi.La vulnerabilità CVE-2021-26855 altera due dei tre parametri RID, ovvero quello di riservatezza e integrità del sistema. In particolare, questa vulnerabilità sui Microsoft Exchange Server consente di eseguire codice da remoto (Remote Code Execution): questa particolare tecnica malevola, combinata con altre vulnerabilità, può avere effetti fatali per i sistemi interessati.L'attacco si suddivide quindi essenzialmente in quattro parti:Si inizia con lo sfruttamento di una vulnerabilità SSRF (Server-Side Request Forgery), documentata appunto come CVE-2021-26855, per inviare richieste HTTP arbitrarie e autenticarsi al server Microsoft Exchange.L'attaccante, quindi, invia payload SOAP, con privilegi

dell’utente SYSTEM sul server Exchange che non sono deserializzati in modo sicuro dal servizio di messaggistica unificata, sfruttando la vulnerabilità CVE-2021-26857.Nella terza fase, dopo l’autenticazione al server grazie allo sfruttamento della CVE-2021-26855, è possibile sfruttare le vulnerabilità: CVE-2021-26858 e CVE-2021-27065. Queste due vulnerabilità fanno parte della catena di attacco e permettono la scrittura di un file in qualunque percorso del sistema di un server Exchange, quindi semplificano il caricamento di altri file malevoli.Nella quarta fase è possibile eseguire azioni per spostarsi lateralmente e cercare di corrompere altri sistemi e/o reti.Seppure l’attacco documentato sia avvenuto in America, l’osservatorio di Exprivia ha rilevato la presenza di 4.362 dispositivi presenti Italia che potrebbero essere affetti da questa vulnerabilità e quindi subire un attacco simile.FiguraLa dislocazione geografica dei server Exchange in Italia potenzialmente vulnerabili. Dati Osservatorio Exprivia Cybersecurity, aggiornati all’11 marzo 2021. Soluzioni per mitigare il rischio di un attacco a Exchange

Per mitigare questa vulnerabilità si consiglia di:limitare le connessioni non attendibili;configurare una VPN per separare il server Exchange dall’accesso esterno. Questo suggerimento ha comunque efficacia solo sulla fase uno dell’attacco, in quanto le altre fasi della kill chain possono essere comunque sfruttate se un attaccante ha già ottenuto l’accesso fraudolento ai sistemi (ad esempio tramite email di phishing). Ecco perché aggiornare i sistemi potrebbe non bastare L’osservatorio di Exprivia ha notato un aumento esponenziale dell’81,9% per le tecniche di phishing e social engineering nel 2020.Si consiglia pertanto di dare la priorità all’installazione degli aggiornamenti sui server Exchange esposti verso l’esterno, in particolare Microsoft Exchange Server 2013, 2016 e 2019 che sono quelli colpiti dalla CVE.È possibile, però, che l’aggiornamento di questi sistemi non basti, infatti se gli attaccanti installassero backdoor su questi sistemi potrebbero accedere nuovamente sfruttando quest’ultime.Dopo questi tipi di attacchi si consiglia di eseguire, dove possibile, una scansione della rete per cercare di capire se tutti i servizi attivi non si comportino in maniera anomala.@RIPRODUZIONE RISERVATA