Ecco le 25 vulnerabilità più usate dagli hacker cinesi secondo l'NSA

Ott 21, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Scenario, Vulnerabilità 0

Un report spiega quali sono i bug sfruttati dai cyber-spioni al soldo del governo di Pechino. La sorpresa? Li conosciamo tutti e ci sono le patch.

Come agiscono gli hacker che operano per conto dei governi e i servizi segreti? Se istintivamente siamo portati a pensare che usino tecniche di attacco estremamente evolute e sconosciute agli esperti di sicurezza, la realtà descrive un altro scenario molto più prosaico.

A confermarlo è la **National Security Agency**, che in un report pubblicato su Internet elenca le vulnerabilità più sfruttate dai gruppi APT cinesi, tra i più pericolosi in circolazione.

Ebbene: nella maggior parte dei casi si tratta di falel di sicurezza ben conosciute e per le quali sono disponibili gli aggiornamenti che le correggono. Ecco l'elenco completo:

1) CVE-2019-11510 – Riguarda i server **Pulse Secure VPN**, in cui un pirata informatico può inviare un URL che avvia una falla per avviare la lettura di file e rubare così la password di accesso.

2) CVE-2020-5902 – La falla interessa I proxies e load balancer **F5 BIG-IP** a livello del **Traffic Management User Interface (TMUI)** cui è affidata la configurazione. La vulnerabilità consente l'esecuzione di codice in remote e, di

conseguenza, la possibilità di assumere il controllo del dispositivo.

3) CVE-2019-19781 – Citrix Application Delivery Controller (ADC) sono vulnerabili a un bug "trasversale" che permette l'esecuzione di codice in remote che aggira il Sistema di autenticazione.

4+5+6) CVE-2020-8193, CVE-2020-8195, CVE-2020-8196 – Le vulnerabilità riguardano sempre Citrix e interessano anche I sistemi SDWAN WAN-OP. Sfruttandoli, è possibile ottenere informazioni sensibili anche attraverso un accesso con un basso livello di privilegi.

7) CVE-2019-0708 – Si tratta del famigerato **BlueKeep** (ne abbiamo parlato in questo articolo) che affligge i sistemi Windows attraverso i servizi Remote Desktop.

8) CVE-2020-15505 – La falla riguarda il software di mobile device management (MDM) **MobileIron**. Sfruttandolo è possible prendere il controllo dei server aziendali.

9) CVE-2020-1350 – Conosciuto come **SigRed** (una descrizione in questo articolo) il bug è rimasto "nascosti" per ben 17 anni.

10) CVE-2020-1472 – La vulnerabilità, battezzata con il nome di **ZeroLogon**, è una delle più recenti emerse in ambiente Windows. I dettagli in questo articolo su **Security Info**.

11) CVE-2019-1040 – Sempre relative ai sistemi Microsoft, il bug consente di portare un attacco Man in The Middle ai danni di NTLM MIC (Message Integrity Check).

12) CVE-2018-6789 – La falla consente di provocare un buffer overflow (e conseguente esecuzione di codice) inviando una mail **Exim**.

13) CVE-2020-0688 – La falla riguarda **Microsoft Exchange** e, in particolare, un problema nella gestione di oggetti a livello di memoria.

14) CVE-2018-4939 – Una vulnerabilità che consente di avviare l'esecuzione di codice in remoto su alcune versioni di **Adobe ColdFusion**.



15) CVE-2015-4852 – I server **Oracle WebLogic 15** soffrono di un bug a livello di un componente (WLS Security che permette di inviare comandi in remoto attraverso oggetti Java.

16) CVE-2020-2555 – Un bug all'interno di **Oracle Coherence** (presente all'interno della suite **Oracle Fusion Middleware**) che permette di compromettere i sistemi.

17) CVE-2019-3396 – La macro **Widget Connector** dei server **Atlassian Confluence 17** permette di iniettare cei modelli che portano all'esecuzione di codice in remoto.

18) CVE-2019-11580 – Il bug interessa **Atlassian Crowd** e I **Crowd Data Center**. Sfruttandolo, è possible installare plugin che permettono di eseguire codice in remote.

19) CVE-2020-10189 – **Zoho ManageEngine Desktop Central** è vulnerabile a un attacco che porta a esecuzione di codice in

remoto.

20) CVE-2019-18935 – Un rischio di esecuzione di codice in remoto a causa di una errata procedura di deserializzazione in **Progress Telerik UI** per **ASP.NET AJAX**.

21) CVE-2020-0601 – **CurveBall** è una falla di sicurezza di Windows che riguarda le **CryptoAPI (Crypt32.dll)** e il modo in cui gestiscono i certificati **Elliptic Curve Cryptography (ECC)**. Sfruttandola, un pirata informatico può creare un falso certificato digitale per un malware.

22) CVE-2019-0803 – La vulnerabilità consente di elevare i privilegi dell'utente nei sistemi Windows.

23) CVE-2017-6327 – Il bug consente di eseguire codice in remote all'interno del **Symantec Messaging Gateway**.

24) CVE-2020-3118 – Il bug interessa l'implementazione del **Cisco Discovery Protocol** implementation in **IOS XR Software**. Le conseguenze consistono in un possible attacco che porta il riavvio del dispositivo o l'esecuzione di codice al suo interno.

25) CVE-2020-8515 – I dispositive **DrayTek Vigor** permettono l'esecuzione di codice in remote con privilege di root attraverso "metacaratteri" vi a shell.

Condividi l'articolo

Hai controllato quali app 0Auth accedono al tuo account Microsoft 365?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/21/ecco-le-25-vulnerabilita-piu-usate-dagli-hacker-cinesi-secondo-lnsa/?utm_source=rss&utm_medium=rss&utm_campaign=ecco-le-25-vulnerabilita-piu-usate-dagli-hacker-cinesi-secondo-lnsa