Oracle, Microsoft, Google: raffica di zero day

Nov 03, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Una vera pioggia di aggiornamenti per correggere vulnerabilità zero day. Aggiornare di corsa: molte vengono già sfruttate dai pirati informatici.

È una settimana particolare, almeno per chi si occupa di sicurezza informatica. A leggere i report pubblicati da vari sviluppatori, infatti, sembra che ci sia un vero boom di vulnerabilità **zero day** per cui è richiesta la massima attenzione.

Partiamo da **Microsoft**, che si trova nella situazione peggiore. A differenza degli altri soggetti coinvolti in questo tsunami di aggiornamenti, infatti, dalle parti di Redmond non hanno ancora messo a disposizione una patch per risolvere la situazione.

La falla di sicurezza (CVE-2020-17087) in questo caso, riguarda i **Windows Kernel Cryptography Driver** e consentirebbe di provocare un crash di sistema. A renderla pubblica il solito **Google Project Zero**, che ha deciso di procedere alla disclosure sulla base del fatto che la falla sarebbe già utilizzata dai cyber criminali.

Nella classifica delle aziende stressate da questo inizio settimana segue Oracle, che si trova a fare i conti con due vulnerabilità "di peso". La prima (CVE-2020-14750) riguarda i server **WebLogic**, che sarebbero soggetti ad attacchi che porterebbero a esecuzione di codice in remoto prima della procedura di autenticazione.

La seconda falla di sicurezza (CVE-2020-14871) riguarda i sistemi **Solaris** e permetterebbe, secondo quanto riportato da **Mandiant** in un report pubblicato su Internet, di aggirare la procedura di autenticazione. La vulnerabilità verrebbe già utilizzata da un gruppo di pirati informatici per diffondere un malware con funzionalità di backdoor.

La "serie terribile" si conclude con una falla individuata in **Chrome** che, anche in questo caso verrebbe già utilizzata in attacchi da parte di pirati informatici. In questo caso la patch c'è, anche se è arrivata dopo la segnalazione dei primi attacchi.

A risentire del bug sarebbe il solito motore **V8**, che nel browser si occupa di gestire **WebAssembly** e **JavaScript**. La falla porterebbe a un buffer overflow (e conseguente possibilità di esecuzione di codice in remoto) sul browser di **Google**.

Insomma: tutti pronti a una bella tornata di aggiornamenti. Speriamo che il resto della settimana riservi meno sorprese…

Condividi l’articolo

L’attacco iraniano sfruttando i siti dei Proud Boys? Ecco i dettagli!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/03/oracle-microsoft-google-raffica-di-zero-day/?utm_source=rss&utm_medium=rss&utm_campaign=oracle-microsoft-google-raffica-di-zero-day