Cybersecurity, Log4Shell: per gli esperti rischio "apocalisse informatica"

Maria Cattini | 14/12/2021 | Sicurezza digitale

Cybersicurezza, Agenzia nazionale avverte: "Vulnerabilità critica Log4Shell"

È come se miliardi di porte di casa fossero improvvisamente aperte, senza più alcuna protezione. Come se chiunque con intenzioni malevole potesse entrarci e prenderne possesso. È ancora difficile stabilire la reale portata della vulnerabilità scoperta sui sistemi informatici che usano il linguaggio Java, ma che si tratti di qualcosa di grave è opinione unanime tra gli esperti. L'**Agenzia per la cyberscicurezza** nazionale parla di "una vasta e diversificata superficie di attacco sulla totalità della rete", definendo la situazione "particolarmente grave". In altre parole, **Internet** è in pericolo. La sua sicurezza è compromessa. A trovarsi improvvisamente col fianco scoperto sono tutti i **software** e le applicazioni scritti in **Java**, il linguaggio di programmazione più usato al mondo: miliardi di programmi e applicazioni, dai server agli **smartphone**. E le conseguenze potrebbero essere ancora peggiori se nei prossimi giorni non si dovessero individuare delle soluzioni a **Log4Shel**l, così è stata chiamata la vulnerabilità, con il rischio di compromettere la sicurezza non solo di **server** e aziende, ma anche dei di **smartphone**, **computer**, insomma, tutti i device in circolazione. Tanto da portare alcuni esperti a parlare di "**Apocalisse informatica**".

Cybersecurity: Log4Shell e rischio di crash globale. L'analisi

Cosa è successo: "I ricercatori hanno scoperto una vulnerabilità in **Log4j**, una libreria usata dalla stragrande maggioranza programmatori di **software** con linguaggio **Java** che consente di scrivere nel software quelli che vengono chiamati 'log', ovvero degli 'status' del software stesso che permettono di fotografare un momento dello sviluppo del software stesso, registrando stati di avanzamento, perfomance, problemi e soluzioni", spiega ad Agi **Marco Ramilli**, amministratore delegato di Yoroi. La vulnerabilità è nei tag di questi log, che un po' come i tag dei blog o quelli su Twitter consentono di individuare il tipo di log che si è scritto in precedenza. "Si è scoperto che uno di questi tag consente consente di eseguire un comando, lanciare un programma", continua Ramilli. Qualsiasi tipo di comando o di programma. Riesce a dire alla macchina: 'Fai questo'. Un attaccante può quindi attraverso questo tag far eseguire alla macchina quello che vuole. Può lanciare codice sulla macchina. Ma per fare cosa? "Qualsiasi cosa. In questo momento quello che vediamo è che gli attaccanti usano questa vulnerabilità per fare attività di mining di criptovalute", ovvero quell'operazione che consente di creare **bitcoin**, attività particolarmente complessa e bisognosa di capacità di calcolo e energia. "Ma potrebbero fare qualsiasi cosa: entrare nei server di un'azienda, vedere quello che c'è dentro, rubare segreti industriali oppure decidere di sferrare degli attacchi ransomware per monetizzare il proprio controllo dei sistemi", ragiona Ramilli, che ammette di aver visto un attacco di questo tipo "circa cinque, otto volte negli ultimi 20 anni".

Log4Shell, cos'é e perchè secondo gli esperti si rischia l'apocalisse informatica

In dettaglio, cos'è **Log4j**? "Se usi Java, probabilmente usi Log4j", spiega ad Agi **Matteo Flora**, esperto di sicurezza informatica e amministratore delegato di TheFool. "È lo standard de facto per chiunque usi Java" per programmare. "È ovunque, dalle Tesla, a Twitter, a Facebook, ai sistemi di controllo numerico fino agli iPhone. Quella che è uscita è una vulnerabilità non ancora risolta". Cosa s□e quindi? "Nel caso peggiore è un po' l'Apocalisse informatica: se non viene risolta questa vulnerabilità si dà la possibilità di lanciare comandi. E già stiamo vedendo in giro criptominer e

accessi abusivi. Il problema è che molta di questa roba è embedded, quindi non ci sono sistemi veloci di aggiornamento. In più è ovunque”. Ramilli invece usa una metafora: “Il logging come quello di Log4j è un po’ come il testo di un attore seguito sul palcoscenico: serve per seguire una traccia, oppure tornare indietro a un punto preciso se si vuole lavorare su un errore”. Una traccia da seguire, e eseguire. In uno dei suoi passaggi però c’è la possibilità di far cambiare completamente trama al testo, e di scriverne una propria. A proprio piacimento.

Cybersicurezza, perché sono a rischio anche smartphone. Allarme hacker

Java è su circa 3 miliardi di dispositivi. E **Log4j**, sviluppato da **Apache**, è usato da quasi tutti i programmatori. Per dare un’idea del suo utilizzo e della sua affidabilità basti pensare che anche Ingenuity, l’elicottero della Nasa atterrato sul suolo di Marte lo scorso febbraio, ha un software che usa Log4j, come la stessa Apache ha reso noto sul proprio profilo Twitter. Ma non c’è bisogno di andare su Marte per capire l’enorme utilizzo di questo linguaggio di programmazione. In queste ore centinaia, forse migliaia di **hacker** in tutto il mondo stanno cercando di individuare nei software e nei server questa vulnerabilità per prenderne possesso e sferrare attacchi. Il rischio più grande al momento lo corrono le aziende e le organizzazioni, più o meno grandi. Situazione resa ancora peggiore dal fatto che spesso è difficile capire se nello sviluppo dei propri software è stato utilizzato Log4j, da chi, e quando. Sulla graticola però non ci sono solo le aziende e le istituzioni. Perché il problema potrebbe presto riguardare anche il singolo utente, un possessore di smartphone, o di uno smartwatch. “Se gli attaccanti attaccano un’azienda, l’utente che è loggato in quel sistema”, che sia Twitter, Minecraft o società di Ecommerce, per citare alcune delle piattaforme che al momento hanno individuato la vulnerabilità, “si potrebbe vedere rubati i propri dati personali, o quelli delle proprie carte di credito”, spiega Ramilli. Mentre ancora più grave è la possibilità che potrebbe verificarsi nei prossimi giorni se non si dovessero trovare soluzioni rapide: “Hacker malevoli potrebbero diffondere link corrotti e aprire tramite questa vulnerabilità delle backdoor sui dispositivi delle persone, telefoni, tablet, qualsiasi oggetto connesso alla rete. E una volta aperta una **backdoor** può fare quello che vuole”. Per Ramilli c’è tempo per qualche giorno ancora. “Già dalla metà della prossima settimana la situazione potrebbe essere difficilmente recuperabile”. Per Log4Shell è una corsa contro il tempo.

Fonte: Affaritaliani
Cybersicurezza, Agenzia nazionale avverte: "Vulnerabilità critica Log4Shell"

È come se miliardi di porte di casa fossero improvvisamente aperte, senza più alcuna protezione. Come se chiunque con intenzioni malevole potesse entrarci e prenderne possesso. È ancora difficile stabilire la reale portata della vulnerabilità scoperta sui sistemi informatici che usano il linguaggio Java, ma che si tratti di qualcosa di grave è opinione unanime tra gli esperti. L’**Agenzia per la cyberscicurezza** nazionale parla di “una vasta e diversificata superficie di attacco sulla totalità della rete”, definendo la situazione “particolarmente grave”. In altre parole, **Internet** è in pericolo. La sua sicurezza è compromessa. A trovarsi improvvisamente col fianco scoperto sono tutti i **software** e le applicazioni scritti in **Java**, il linguaggio di programmazione più usato al mondo: miliardi di programmi e applicazioni, dai server agli **smartphone**. E le conseguenze potrebbero essere ancora peggiori se nei prossimi giorni non si dovessero individuare delle soluzioni a **Log4Shel**l, così è stata chiamata la vulnerabilità, con il rischio di compromettere la sicurezza non solo di **server** e aziende, ma anche dei di **smartphone**, **computer**, insomma, tutti i device in circolazione. Tanto da portare alcuni esperti a parlare di “**Apocalisse informatica**”.

Cybersecurity: Log4Shell e rischio di crash globale. L'analisi

Cosa è successo: “I ricercatori hanno scoperto una vulnerabilità in **Log4j**, una libreria usata dalla stragrande maggioranza programmatori di **software** con linguaggio **Java** che consente di scrivere nel software quelli che vengono chiamati ‘log’, ovvero degli ‘status’ del software stesso che permettono di fotografare un momento dello sviluppo del software stesso, registrando stati di avanzamento, perfomance, problemi e soluzioni”, spiega ad Agi **Marco Ramilli**, amministratore delegato di Yoroi. La vulnerabilità è nei tag di questi log, che un po’ come i tag dei blog o quelli su Twitter consentono di individuare il tipo di log che si è scritto in precedenza. “Si è scoperto che uno di questi tag consente consente di eseguire un comando, lanciare un programma”, continua Ramilli. Qualsiasi tipo di comando o di programma. Riesce a dire alla macchina: ‘Fai questo’. Un attaccante può quindi attraverso questo tag far eseguire alla macchina quello che vuole. Può lanciare codice

sulla macchina. Ma per fare cosa? “Qualsiasi cosa. In questo momento quello che vediamo è che gli attaccanti usano questa vulnerabilità per fare attività di mining di criptovalute”, ovvero quell’operazione che consente di creare **bitcoin**, attività particolarmente complessa e bisognosa di capacità di calcolo e energia. “Ma potrebbero fare qualsiasi cosa: entrare nei server di un’azienda, vedere quello che c’è dentro, rubare segreti industriali oppure decidere di sferrare degli attacchi ransomware per monetizzare il proprio controllo dei sistemi”, ragiona Ramilli, che ammette di aver visto un attacco di questo tipo “circa cinque, otto volte negli ultimi 20 anni”.

Log4Shell, cos'é e perchè secondo gli esperti si rischia l'apocalisse informatica

In dettaglio, cos’è **Log4j**? “Se usi Java, probabilmente usi Log4j”, spiega ad Agi **Matteo Flora**, esperto di sicurezza informatica e amministratore delegato di TheFool. “È lo standard de facto per chiunque usi Java” per programmare. “È ovunque, dalle Tesla, a Twitter, a Facebook, ai sistemi di controllo numerico fino agli iPhone. Quella che è uscita è una vulnerabilità non ancora risolta”. Cosa s□e quindi? “Nel caso peggiore è un po’ l’Apocalisse informatica: se non viene risolta questa vulnerabilità si dà la possibilità di lanciare comandi. E già stiamo vedendo in giro criptominer e accessi abusivi. Il problema è che molta di questa roba è embedded, quindi non ci sono sistemi veloci di aggiornamento. In più è ovunque”. Ramilli invece usa una metafora: “Il logging come quello di Log4j è un po’ come il testo di un attore seguito sul palcoscenico: serve per seguire una traccia, oppure tornare indietro a un punto preciso se si vuole lavorare su un errore”. Una traccia da seguire, e eseguire. In uno dei suoi passaggi però c’è la possibilità di far cambiare completamente trama al testo, e di scriverne una propria. A proprio piacimento.

Cybersicurezza, perché sono a rischio anche smartphone. Allarme hacker

Java è su circa 3 miliardi di dispositivi. E **Log4j**, sviluppato da **Apache**, è usato da quasi tutti i programmatori. Per dare un’idea del suo utilizzo e della sua affidabilità basti pensare che anche Ingenuity, l’elicottero della Nasa atterrato sul suolo di Marte lo scorso febbraio, ha un software che usa Log4j, come la stessa Apache ha reso noto sul proprio profilo Twitter. Ma non c’è bisogno di andare su Marte per capire l’enorme utilizzo di questo linguaggio di programmazione. In queste ore centinaia, forse migliaia di **hacker** in tutto il mondo stanno cercando di individuare nei software e nei server questa vulnerabilità per prenderne possesso e sferrare attacchi. Il rischio più grande al momento lo corrono le aziende e le organizzazioni, più o meno grandi. Situazione resa ancora peggiore dal fatto che spesso è difficile capire se nello sviluppo dei propri software è stato utilizzato Log4j, da chi, e quando. Sulla graticola però non ci sono solo le aziende e le istituzioni. Perché il problema potrebbe presto riguardare anche il singolo utente, un possessore di smartphone, o di uno smartwatch. “Se gli attaccanti attaccano un’azienda, l’utente che è loggato in quel sistema”, che sia Twitter, Minecraft o società di Ecommerce, per citare alcune delle piattaforme che al momento hanno individuato la vulnerabilità, “si potrebbe vedere rubati i propri dati personali, o quelli delle proprie carte di credito”, spiega Ramilli. Mentre ancora più grave è la possibilità che potrebbe verificarsi nei prossimi giorni se non si dovessero trovare soluzioni rapide: “Hacker malevoli potrebbero diffondere link corrotti e aprire tramite questa vulnerabilità delle backdoor sui dispositivi delle persone, telefoni, tablet, qualsiasi oggetto connesso alla rete. E una volta aperta una **backdoor** può fare quello che vuole”. Per Ramilli c’è tempo per qualche giorno ancora. “Già dalla metà della prossima settimana la situazione potrebbe essere difficilmente recuperabile”. Per Log4Shell è una corsa contro il tempo.

Fonte: Affaritaliani