Olympus Winter & Ibe GmbH, Kuehnstraße 61, 22045 Amburgo

A chi di competenza

Data
30.07.2021

**"PrintNightmare":**
**vulnerabilità all'esecuzione di codice remoto nello spooler di stampa di Windows**

Gentili Signore e Signori,

è stata rilevata una vulnerabilità critica nel servizio spooler di stampa di Windows. Questa vulnerabilità è stata denominata "PrintNightmare". Microsoft ha assegnato il numero **CVE-2021-1675** a questa vulnerabilità.

Il 29 giugno 2021 hanno cominciato a circolare gli exploit per questa vulnerabilità. Microsoft ha assegnato un secondo numero a questa vulnerabilità: **CVE-2021-34527**.

Il 7 luglio 2021, Microsoft ha pubblicato degli aggiornamenti esterni alla banda per alcune versioni (ma non tutte) di Windows. Secondo l'avvertenza aggiornata di Microsoft, "gli aggiornamenti di sicurezza rilasciati il 6 luglio 2021 e nei giorni successivi contengono protezioni per la CVE-2021-1675 e per l'exploit aggiuntivo dell'esecuzione di codice remoto nel servizio spooler di stampa di Windows conosciuto come 'PrintNightmare, documentato nel CVE-2021-34527". È stato rilevato uno sfruttamento in circolazione e TUTTI i sistemi Windows ne sono interessati.

Il 15 luglio 2021, Microsoft ha assegnato un terzo numero alla vulnerabilità "PrintNightmare": **CVE-2021-34481**. Al momento non si è ancora a conoscenza di un exploit pubblico per questa vulnerabilità.

**Dispositivi OSTE interessati**

Tutte le versioni dei seguenti prodotti OSTE includono una versione di Windows e sono interessati dalla vulnerabilità “PrintNightmare”:

- VMC-3
- VMC-7
- VMC-10
- VMC-30.

OSTE ha rilasciato il Bollettino di assistenza tecnica SBU_100-219-293 per prendere in esame la vulnerabilità “PrintNightmare” su tali prodotti. Questo Bollettino di assistenza tecnica contiene istruzioni per i tecnici dell’assistenza destinate all’esecuzione dell’arresto e disabilitazione del servizio spooler di stampa di Windows per VMC-3, VMC-7, VMC-10 e VMC-30. La disabilitazione del servizio spooler di stampa di Windows rappresenta una soluzione rapida ed efficace per chiudere la vulnerabilità “PrintNightmare” in Windows.

Contattare l’assistenza Olympus per ottenere le azioni correttive definite nel Bollettino dell’assistenza tecnica applicate sul proprio VMC.

**Altri prodotti OSTE**

OSTE, tra l’altro, produce e fornisce software che devono essere installati su computer con sistema operativo Windows:

- ENDOBASE
- Hytrack

Dato l’alto rischio comportato dalla vulnerabilità “PrintNightmare”, OSTE consiglia vivamente di applicare le istruzioni di correzione che seguono al fine di ridurre al minimo il rischio causato dalla vulnerabilità PrintNightmare.

**Raccomandazioni generali**

La vulnerabilità PrintNightmare interessa tutti i tipi e tutte le versioni di Windows, ovvero sia le installazioni client che server.

Se un computer Windows non necessita della funzionalità di stampa, OSTE raccomanda di arrestare e disabilitare il servizio spooler di stampa di Windows su tali computer. La disabilitazione del servizio spooler di stampa corregge la vulnerabilità “PrintNightmare” su tutti i tipi e tutte le versioni di Windows. Però disabilita anche la possibilità di stampare da un computer.

Nei server Hytrack, la funzionalità di stampa è necessaria per l’esecuzione della stampa automatica di protocolli di ricondizionamento e, su client Hytrack, per la stampa manuale dei protocolli.

Sui server ENDOBASE, la funzionalità di stampa non è necessaria.

Per quanto riguarda il numero CVE associato a “PrintNightmare”, CVE-2021-34481, la disabilitazione del servizio spooler di stampa è l’unica soluzione temporanea fornita da Microsoft alla data di rilascio di questo documento (luglio 2021).

Ulteriori informazioni sono disponibili alla pagina Web Microsoft per il CVE-2021-34481:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

Se è necessario utilizzare la funzione di stampa su un computer, l’azione correttiva raccomandata varia in base alla versione di Windows.

**Versioni Windows 10 e server basati su Windows 10**

Microsoft ha pubblicato degli aggiornamenti di sicurezza per tutte le versioni di Windows 10 e delle versioni server correlate. Per informazioni dettagliate e link relativi agli articoli Knowledge Base, consultare la pagina Web Microsoft per il CVE-2021-34527:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Per rendere sicuro il proprio sistema, oltre ad eseguire l’installazione degli aggiornamenti, è necessario confermare che le seguenti impostazioni di registro non siano definite o che siano impostate su 0 (zero):

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)`
- `UpdatePromptSettings = 0 (DWORD) or not defined (default setting)`

L’impostazione di `NoWarningNoElevationOnInstall` su 1 rende il proprio sistema intrinsecamente vulnerabile.

**Windows 7 e versioni server basate su Windows 7**

Microsoft ha pubblicato degli aggiornamenti di sicurezza per le versioni Windows 7 e server basati su Windows 7 solo per i clienti in possesso di un contratto Extended Support Update (ESU).

Se l’opzione di disabilitazione del servizio spooler di stampa non è fattibile, sussistono delle soluzioni temporanee che permettono di ridurre il rischio creato dalla vulnerabilità “PrintNightmare”.

**Disabilitazione della stampa remota in ingresso tramite Criteri di gruppo**

Configurare le impostazioni tramite Criteri di gruppo come segue:

`Computer Configuration / Administrative Templates / Printers`

Disabilitare il criterio “`Allow Print Spooler to accept client connections`” per bloccare gli attacchi remoti.

Per applicare questo criterio di gruppo, occorre riavviare il servizio spooler di stampa.

Informazioni dettagliate sono disponibili alla pagina Web Microsoft per il CVE-2021-34527:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

**Limitazione dell'installazione di nuovi driver per stampante (impostazioni di Selezione e stampa)**

In assenza di installazione dell'aggiornamento di sicurezza, al fine di mitigare il rischio creato dalla vulnerabilità "PrintNightmare" si raccomandano le seguenti impostazioni:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)`
- `UpdatePromptSettings = 0 (DWORD) or not defined (default setting)`

L'impostazione di `NoWarningNoElevationOnInstall` su 1 rende il proprio sistema intrinsecamente vulnerabile.

Cordiali saluti

Alois Baier
Responsabile Sicurezza di prodotto
R&D | Sicurezza di prodotto