Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Impatto della vulnerabilità CVE-2021-39238 sulle certificazioni dei dispositivi HP rilasciate dall'OCSI

28 febbraio 2022

1 Riferimenti

[CEM] CCMB-2017-04-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 5, April 2017

[CVE] NIST NVD: CVE-2021-39238 Detail (https://nvd.nist.gov/vuln/detail/CVE-2021-39238)

[FSAD] F-Secure Advisory: "HP Multi-Function Printers - Improper validation of an array index" (https://labs.f-secure.com/advisories/hp-multi-function-printers-improper-validation-of-an-array-index/)

[FSRP] F-Secure Lab Research Paper: "Printing Shellz", Alexander Bolshev e Timo Hirvonen, 30 novembre 2021 (https://labs.f-secure.com/publications/printing-shellz)

[HPSB] HP Customer Support - Knowledge Base: "Certain HP LaserJet, LaserJet Managed, PageWide, PageWide Managed printers - Potential buffer overflow", HPSBPI03749, 1 novembre 2021 (https://support.hp.com/us-en/document/ish_5000383-5000409-16)

2 Introduzione

L'Organismo di Certificazione della Sicurezza Informatica (OCSI) è stato recentemente informato della presenza di una vulnerabilità critica (CVE-2021-39238 [CVE]) in diversi dispositivi prodotti dalla società HP Inc. (stampanti multi-funzione, stampanti a funzione singola, scanner).

Alcuni di questi prodotti sono stati certificati dall'OCSI nell'ambito dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT.

Scopo del presente documento è quello di analizzare l'impatto della vulnerabilità in oggetto sulle certificazioni dei dispositivi HP attualmente in corso di validità.

3 Descrizione della vulnerabilità

Si tratta di una vulnerabilità di tipo *buffer overflow* che potrebbe potenzialmente essere sfruttata per eseguire codice arbitrario da remoto sui sistemi affetti.

A questa vulnerabilità è stato assegnato il codice CVE-2021-39238 ed uno score CVSSv3 pari a 9.8 (*Critical*). Per maggiori dettagli si rimanda alla voce corrispondente nel National Vulnerability Database del NIST ([CVE]).

La vulnerabilità è stata scoperta e divulgata da ricercatori di sicurezza della società F-Secure ([FSAD], [FSRP]). Stando a quanto riportato dagli autori della ricerca, la vulnerabilità risiede all'interno del firmware dei dispositivi HP affetti. In particolare, la libreria del *parser* dei caratteri è vulnerabile a un problema di corruzione della memoria causato da una convalida impropria di un indice di matrice.

Se sfruttata con successo, questa vulnerabilità può consentire a un attaccante locale o remoto di ottenere il controllo sul software della stampante, entrare in possesso di documenti che vengono scansionati o stampati o propagarsi attraverso l'infrastruttura di rete. La vulnerabilità può essere sfruttata in diversi modi: stampando un documento da USB, stampando da un messaggio di posta elettronica, richiamando la funzione di stampa da un browser utilizzando codice JavaScript su una pagina Web appositamente predisposta o comunicando direttamente sulla porta TCP 9100 (JetDirect).

Secondo il bollettino di sicurezza pubblicato da HP ([HPSB]), questa vulnerabilità affligge circa 150 modelli di stampanti e scanner, anche se la sua effettiva sfruttabilità è stata dimostrata da F-Secure solamente sulla stampante HP LaserJet Enterprise MFP M725z.

HP ha già provveduto a rilasciare versioni del firmware aggiornate per i prodotti potenzialmente affetti.

4 Modelli di dispositivi HP certificati affetti dalla vulnerabilità

Sulla base di informazioni richieste dall'OC direttamente al produttore HP Inc., è stato riscontrato che tutti i modelli di dispositivi HP certificati da OCSI alla data del presente documento, elencati in Tabella 1, risultano affetti dalla vulnerabilità CVE-2021-39238.

Numero certificato	Nome modello	Codice prodotto	Vers. firmware di Sistema	Vers. firmware JetDirect Inside
6/20	HP Color LaserJet Enterprise MFP M776dn	T3U55A	2410028_055041	JSI24100002
6/20	HP Color LaserJet Enterprise Flow MFP M776z	3WT91A	2410028_055041	JSI24100002
6/20	HP Color LaserJet Enterprise Flow MFP M776zs	T3U56A	2410028_055041	JSI24100002
6/20	HP LaserJet Enterprise MFP M632z	J8J72A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M633z	J8J78A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M634dn	7PS94A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M634h	7PS95A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M634z	7PS96A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M635fht	7PS98A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M635h	7PS97A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M635z	7PS99A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M636fh	7PT00A	2410028_055025	JSI24100002
6/20	HP LaserJet Enterprise MFP M636z	7PT01A	2410028_055025	JSI24100002
6/20	HP LaserJet Managed MFP E62655dn	3GY14A	2410028_055025	JSI24100002
6/20	HP LaserJet Managed MFP E62665hs	3GY15A	2410028_055025	JSI24100002

Numero certificato	Nome modello	Codice prodotto	Vers. firmware di Sistema	Vers. firmware JetDirect Inside
6/20	HP LaserJet Managed MFP Flow E62665h	3GY16A	2410028_055025	JSI24100002
6/20	HP LaserJet Managed MFP Flow E62665z	3GY17A	2410028_055025	JSI24100002
6/20	HP LaserJet Managed MFP Flow E62675z	3GY18A	2410028_055025	JSI24100002
6/20	HP Color LaserJet Enterprise MFP Flow M681z	J8A13A	2410028_055026	JSI24100002
6/20	HP Color LaserJet Enterprise MFP Flow M682z	J8A17A	2410028_055026	JSI24100002
6/20	HP Color LaserJet Managed MFP E67650dh	3GY31A	2410028_055026	JSI24100002
6/20	HP Color LaserJet Managed Flow MFP E67660z	3GY32A	2410028_055026	JSI24100002
7/20	HP Color LaserJet Enterprise M856dn	T3U51A	2410028_055002	JSI24100002
7/20	HP Color LaserJet Enterprise M856x	T3U52A	2410028_055002	JSI24100002
7/20	HP Color LaserJet Managed E85055dn	T3U66A	2410028_055002	JSI24100002
7/20	HP Color LaserJet Managed E55040dn	3GX99A	2410028_055028	JSI24100002
7/20	HP LaserJet Enterprise M607n	K0Q14A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M607dn	K0Q15A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M608n	K0Q17A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M608dn	K0Q18A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M608x	K0Q19A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M609dn	K0Q21A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M609dh	K0Q20A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M609x	K0Q22A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M610dn	7PS82A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M611dn	7PS84A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M611x	7PS85A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M612dn	7PS86A	2410028_055009	JSI24100002
7/20	HP LaserJet Enterprise M612x	7PS87A	2410028_055009	JSI24100002
4/21	HP PageWide Enterprise Color Flow MFP 785zs	J7Z12A	2411097_060485	JSI24110014
4/21	HP PageWide Enterprise Color Flow MFP 785z+	Z5G75A	2411097_060485	JSI24110014
4/21	HP PageWide Managed Color Flow MFP E77650z+	Z5G76A	2411097_060485	JSI24110014
4/21	HP PageWide Managed Color Flow MFP E77660z+	Z5G78A	2411097_060485	JSI24110014
4/21	HP PageWide Enterprise Color MFP 586z	G1W41A	2411097_060472	JSI24110014
4/21	HP LaserJet Managed MFP E52545dn	3GY19A	2411097_060468	JSI24110014
4/21	HP LaserJet Managed MFP Flow E52545c	3GY20A	2411097_060468	JSI24110014
4/21	HP Color LaserJet Managed MFP E57540dn	3GY25A	2411097_060474	JSI24110014
4/21	HP Color LaserJet Managed MFP E57540c	3GY26A	2411097_060474	JSI24110014
4/21	HP LaserJet Enterprise MFP M528dn	1PV64A	2411097_060496	JSI24110014

Numero certificato	Nome modello	Codice prodotto	Vers. firmware di Sistema	Vers. firmware JetDirect Inside
4/21	HP LaserJet Enterprise MFP M528f	1PV65A	2411097_060496	JSI24110014
4/21	HP LaserJet Enterprise MFP M528c	1PV66A	2411097_060496	JSI24110014
4/21	HP LaserJet Enterprise MFP M528z	1PV67A	2411097_060496	JSI24110014
4/21	HP LaserJet Managed MFP E52645dn	1PS54A	2411097_060496	JSI24110014
4/21	HP LaserJet Managed MFP E52645c	1PS55A	2411097_060496	JSI24110014
6/21	HP LaserJet Enterprise M507dn	1PV87A	2411097_060463	JSI24110014
6/21	HP LaserJet Enterprise M507dng	1PV89A	2411097_060463	JSI24110014
6/21	HP Color LaserJet Enterprise M751n	T3U43A	2411097_060467	JSI24110014
6/21	HP Color LaserJet Enterprise M751dn	T3U44A	2411097_060467	JSI24110014
6/21	HP Color LaserJet Managed E75245dn	T3U64A	2411097_060467	JSI24110014
7/21	HP ScanJet Enterprise Flow N9120 fn2 Document Scanner	L2763A	2411097_060492	JSI24110014
7/21	HP Digital Sender Flow 8500 fn2 Document Capture Workstation	L2762A	2411097_060482	JSI24110014

Tabella 1 – Elenco dei modelli di dispositivi HP certificati da OCSI affetti dalla vulnerabilità CVE-2021-39238

5 Impatto sulle certificazioni in corso di validità

Come si può dedurre dalla Tabella 1, i certificati OCSI coinvolti sono i seguenti:

- Certificato num. 6/20 emesso in data 8 settembre 2020
- Certificato num. 7/20 emesso in data 8 settembre 2020
- Certificato num. 4/21 emesso in data 19 luglio 2021
- Certificato num. 6/21 emesso in data 23 settembre 2021
- Certificato num. 7/21 emesso in data 23 settembre 2021

L'Organismo di Certificazione (OCSI) ha incaricato il laboratorio (LVS) che ha effettuato le attività di valutazione per tutte le certificazioni sopra elencate (atsec information security S.r.l. con sede in Roma) di condurre un'analisi di impatto volta a determinare l'effettiva applicabilità della vulnerabilità CVE-2021-39238 agli ODV certificati. Un'ulteriore analisi è stata effettuata internamente dall'OC.

L'analisi effettuata ha portato a individuare svariati fattori di mitigazione che limitano notevolmente la superficie di attacco esposta dai dispositivi certificati. In particolare, le seguenti funzionalità sono disattivate nella configurazione valutata:

- Device USB e Host USB *plug and play*
- HP Web Services (ePrint)
- Funzionalità wireless (NFC, BLE, Wireless Direct Print, Wireless station, AirPrint)
- Internet Printing Protocol (IPP/IPPS) e LPD
- Web Services Print
- EWS print page

Inoltre, le comunicazioni HTTP(S) e sulla porta TCP 9100 sono protette da IPsec. I dispositivi devono essere posti dietro un firewall e non sono connessi ad Internet.

In pratica, l'unico metodo di stampa disponibile nella configurazione certificata è tramite connessione cablata sulla porta TCP 9100. Solo i computer autorizzati e autenticati su questa porta tramite IPsec possono inviare documenti da stampare ai dispositivi presenti sulla stessa LAN.

Con queste ipotesi, l'unica possibilità per un attaccante di sfruttare la vulnerabilità CVE-2021-39238 resta quella di indurre un utente autorizzato a stampare su un dispositivo affetto un documento malevolo appositamente predisposto, fatto recapitare sul suo PC ad esempio tramite un'Email di *phishing*.

Di norma, un simile scenario di attacco risulta mirato ad un obiettivo ben definito, in quanto richiede un buon livello di organizzazione e pianificazione. Si presume che l'attaccante sia fortemente motivato, sia a conoscenza della presenza di dispositivi vulnerabili all'interno dell'infrastruttura di rete dell'azienda bersaglio e sia in grado di individuare una o più potenziali vittime tra il personale autorizzato.

A questo va aggiunto che l'attaccante deve essere in grado di sviluppare un *exploit* specifico per la vulnerabilità CVE-2021-39238. Al momento, nonostante i dettagli della vulnerabilità siano stati divulgati da F-Secure, non si ha notizia di *exploit* pubblicamente disponibili.

Sulla base delle informazioni disponibili, l'LVS ha provveduto altresì a calcolare il potenziale di attacco necessario per sfruttare la vulnerabilità CVE-2021-39238, che è risultato pari a Enhanced-Basic. Il calcolo è riportato in Appendice A – Calcolo del potenziale d'attacco.

6 Conclusioni e raccomandazioni

In considerazione della ridotta superficie di attacco nella configurazione valutata e del potenziale di attacco richiesto (**Enhanced-Basic**) per poter essere sfruttata con successo, la vulnerabilità CVE-2021-39238 è da considerarsi applicabile ma **residua** per i dispositivi certificati elencati in Tabella 1.

Pertanto, i certificati emessi finora da OCSI per i dispositivi HP coinvolti, elencati nel cap. 5, mantengono la loro validità.

Ciò nonostante, si raccomanda agli utilizzatori dei dispositivi HP affetti dalla vulnerabilità CVE-2021-39238 di installare al più presto la versione aggiornata del firmware che risolve questa vulnerabilità. Per maggiori dettagli sugli aggiornamenti disponibili e per i link di download si faccia riferimento al bollettino di sicurezza di HP ([HPSB]).

7 Appendice A – Calcolo del potenziale d'attacco

In Tabella 2 è riportato il calcolo del potenziale di attacco richiesto per sfruttare la vulnerabilità CVE-2021-39238 su un dispositivo HP certificato nella sua configurazione valutata e nell'ambiente operativo previsto. Il calcolo è stato effettuato sulla base delle indicazioni fornite nel par. B.4 della Common Evaluation Methodology dei Common Criteria ([CEM]).

Fattore	Valore	Commento
Elapsed time	4	Sono necessarie più di due settimane per progettare un exploit del *buffer overflow* scoperto da F-Secure e quindi armarlo con un altro exploit che violi il TSF dell'ODV. Il solo sfruttamento del *buffer overflow* per causare il blocco del dispositivo (Denial of Service) non è sufficiente.
Specialist expertise	6	Richiede un'ottima conoscenza dei meccanismi di *buffer overflow*; inoltre, anche se la ricerca di F-Secure spiega la procedura in dettaglio, è comunque richiesta una certa esperienza per la riproduzione dell'exploit.
Knowledge of the TOE	0	È sufficiente la conoscenza di informazioni di pubblico dominio.
Window of opportunity	0	Non è necessario un accesso diretto all'ODV.
IT hardware/software or other equipment	2	Oltre agli strumenti standard (PC, compilatori, ecc.) sono necessari strumenti software avanzati e specifici per il firmware dei dispositivi HP.
Totale	**12**	**Potenziale di attacco richiesto = Enhanced-Basic**

Tabella 2 - Calcolo del potenziale d'attacco richiesto per sfruttare la vulnerabilità CVE-2021-39238