TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2017-115

DATE(S) ISSUED: 11/27/2017

SUBJECT: A Vulnerability in HP Products Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in HP Products, which could allow for arbitrary code execution. Depending on the printer's placement on the network, an attacker could potentially install programs; view, change, or delete data; or create new accounts with full user rights. Printers whose administrative account logins have been changed could be less impacted than those systems with default administrative credentials.

THREAT INTELLIGENCE:
There is no evidence of this vulnerability being exploited in the wild. However, the MS-ISAC has previously observed a variety of printer exploits and defacements affecting Internet-facing printers in state, local, tribal, and territorial governments, especially those located in universities, K-12 schools, and fire stations.

SYSTEMS AFFECTED:
- HP Color LaserJet Enterprise M651CZ255A, CZ256A, CZ257A, CZ258A firmware versions prior to 2405129_000047
- HP Color LaserJet Enterprise M652J7Z98A, J7Z99A firmware versions prior to 2405130_000068
- HP Color LaserJet Enterprise M653J8A04A, J8A05A, J8A06A firmware versions prior to 2405130_000068
- HP Color LaserJet Enterprise MFP M577B5L46A, B5L47A, B5L48A firmware versions prior to 2405129_000038
- HP Color LaserJet Enterprise M552B5L23A, B5L23 firmware versions prior to 2308903_577315
- HP Color LaserJet Enterprise M553B5L24A, B5L25A, B5L26A, B5L27A, B5L38A firmware versions prior to 2308903_577315
- HP Color LaserJet M680CZ250A, CA251A firmware versions prior to 2405129_000042
- HP Color LaserJet Managed E65050L3U55A firmware versions prior to 2405130_000068
- HP Color LaserJet Managed E65060L3U56A, L3U57A firmware versions prior to 2405130_000068
- HP LaserJet Enterprise 500 color MFP M575CD644A, CD645A firmware versions prior to 2405129_000045
- HP LaserJet Enterprise 500 MFP M525CF116A, CF117A firmware versions prior to 2405129_000048
- HP LaserJet Enterprise 700 color MFP M775CF304A, CC523A, CC524C, CC522A, L3U49A, L3U50A firmware versions prior to 2405129_000061
- HP LaserJet Enterprise 800 color M855A2W77A, A2W78A, A2W79A firmware versions prior to 2405129_000057
- HP LaserJet Enterprise 800 color MFP M880A2W76A, A2W75A, D7P70A, D7P71A firmware versions prior to 2405129_000054
- HP LaserJet Enterprise color flow MFP M575CD646A firmware versions prior to 2405129_000045
- HP LaserJet Enterprise flow M830z MFPCF367A firmware versions prior to 2405129_000060
- HP LaserJet Enterprise flow MFP M525CF118A firmware versions prior to 2405129_000048
- HP LaserJet Enterprise Flow MFP M630B3G85A firmware versions prior to 2405129_000040
- HP LaserJet Enterprise Flow MFP M631J8J64A firmware versions prior to 2405129_000041
- HP LaserJet Enterprise Flow MFP M632J8J72A firmware versions prior to 2405129_000041
- HP LaserJet Enterprise Flow MFP M633J8J78A firmware versions prior to 2405129_000041
- HP LaserJet Enterprise M527F2A76A, F2A77A, F2A81A firmware versions prior to 2405129_000039
- HP LaserJet Enterprise M607K0Q14A, K0Q15A firmware versions prior to 2405130_000069
- HP LaserJet Enterprise M608K0Q17A, K0Q18A, M0P32A, K0Q19A firmware versions prior to 2405130_000069
- HP LaserJet Enterprise M609K0Q20A, K0Q21A, K0Q22A firmware versions prior to 2405130_000069
- HP LaserJet Enterprise M806CZ244A, CZ245A firmware versions prior to 2405129_000059

- HP LaserJet Enterprise MFP M630J7X28A firmware versions prior to 2405129_000040
- HP LaserJet Enterprise MFP M631J8J63A, J8J65A firmware versions prior to 2405129_000041
- HP LaserJet Enterprise MFP M632J8J70A, J8J71A firmware versions prior to 2405129_000041
- HP LaserJet Enterprise MFP M633J8J76A firmware versions prior to 2405129_000041
- HP LaserJet Enterprise MFP M725CF066A, CF067A, CF068A, CF069A firmware versions prior to 2405129_000058
- HP LaserJet Managed E60055M0P33A firmware versions prior to 2405130_000069
- HP LaserJet Managed E60065M0P35A, M0P36A firmware versions prior to 2405130_000069
- HP LaserJet Managed E60075M0P39A, M0P40A firmware versions prior to 2405130_000069
- HP LaserJet Managed Flow MFP E62555J8J67A firmware versions prior to 2405129_000041
- HP LaserJet Managed Flow MFP E62565J8J74A, J8J79A firmware versions prior to 2405129_000041
- HP LaserJet Managed Flow MFP E62575J8J80A firmware versions prior to 2405129_000041
- HP LaserJet Managed MFP E62555J8J66A firmware versions prior to 2405129_000041
- HP LaserJet Managed MFP E62565J8J73A firmware versions prior to 2405129_000041
- HP OfficeJet Enterprise Color Flow MFP X585B5L06A, B5L06, ,B5L07A firmware versions prior to 2405129_000050
- HP OfficeJet Enterprise Color MFP X585B5L04A, B5L04, B5L05A, B5L05 firmware versions prior to 2405129_000050
- HP PageWide Enterprise Color 765J7Z04A firmware versions prior to 2405087_018564
- HP PageWide Enterprise Color MFP 586G1W39A, G1W39, G1W40A, G1W40 firmware versions prior to 2405129_000066
- HP PageWide Enterprise Color MPF 780J7Z09A, J7Z10A firmware versions prior to 2405087_018548
- HP PageWide Enterprise Color MPF 785J7Z11A, J7Z12A firmware versions prior to 2405087_018548
- HP PageWide Enterprise Color X556G1W46A, G1W46, G1W47A, G1W47, L3U44A firmware versions prior to 2405129_000051
- HP PageWide Managed Color E55650L3U44A firmware versions prior to 2405129_000051
- HP PageWide Managed Color E75160J7Z06A firmware versions prior to 2405087_018564
- HP PageWide Managed Color Flow MFP 586G1W41A, G1W41 firmware versions prior to 2405129_000066
- HP PageWide Managed Color Flow MFP E77650J7Z08A, J7Z14A firmware versions prior to 2405087_018548
- HP PageWide Managed Color Flow MFP E77660Z5G77A, J7Z03A, J7Z07A, J7Z05A firmware versions prior to 2405087_018548
- HP PageWide Managed Color MFP E77650J7Z13A, Z5G79A firmware versions prior to 2405087_018548
- HP ScanJet Enterprise Flow N9120 Doc Flatbed ScannerL2683A firmware versions prior to 2405087_018552
- HP Digital Sender Flow 8500 fn2 Doc Capture WorkstationL2762A firmware versions prior to 2405087_018553

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in HP products which could allow for arbitrary code execution due to insufficient DLL signature validation. Depending on the printer's placement on the network, an attacker could potentially install programs; view, change, or delete data; or create new accounts with full user rights. Printers whose administrative account logins have been changed could be less impacted than those systems with default administrative credentials.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by HP to vulnerable systems, immediately after appropriate testing.
- Change all default printer login credentials and/or passwords.
- Implement the same security policies for printers as would be implemented on any networked system.
- Restrict inbound access to only authorized IP addresses, machines, and/or users.
- Disable unnecessary functions, services, and/or ports.
- Log printer activity and connections, and retain logs for a minimum of 90 days.
- Implement security features offered by printer manufacturers that include measures such as hard drive encryption, automated deletion of printer jobs, and drive overwrite capabilities.

REFERENCES:

HP:
https://support.hp.com/nz-en/document/c05839270

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2750

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722