TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-087

DATE(S) ISSUED: 08/07/2018

SUBJECT: Multiple Vulnerabilities in HP Printer Products Could Allow for Remote Code Execution

OVERVIEW:
Multiple Vulnerabilities have been discovered in HP Printer products, which could allow for remote 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.

THREAT INTELLIGENCE:
There is no evidence of these vulnerabilities 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:
Refer to the list in the HP Security Bulletin for the full list of affected printer systems

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: High

TECHNICAL SUMMARY:
Multiple Vulnerabilities have been discovered in HP products, which could allow for remote code execution. An attacker can exploit these vulnerabilities by sending a maliciously crafted file to an affected device which can cause a stack or static buffer overflow (CVE-2018-5924, CVE-2018-5925). 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.

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/us-en/document/c06097712

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5924
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5925

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