Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Schwachstellen in HP Multifunktionsdruckern

CSW-Nr. 2021-548868-1033, Version 1.0, 01.12.2021

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:GREEN: Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisation und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Die Sicherheitsforscher Timo Hirvonen und Alexander Bolshev von F-Secure haben wurmfähige Schwachstellen im physischen Zugriffsport (CVE-2021-39237) sowie im Font-Parsing (CVE-2021-39238) von HP-Multifunktionsdruckern entdeckt [FSE2021a]. Angreifer können die Schwachstellen ausnutzen, um die Kontrolle über ungeschützte Multifunktionsdrucker zu erlangen, Informationen zu stehlen und Netzwerke so zu infiltrieren, dass weiterer Schaden angerichtet werden kann. Obwohl verschiedene Angriffsszenarien denkbar sind (z.B. Drucken via speziell präparierter USB-Sticks oder direkt über den physischen LAN-Port), erscheint ein sogenannter Cross-Site-Printing (XSP) Angriff für Angreifer die attraktivste Methode zu sein. Dabei werden Mitarbeitende eines Unternehmens, z.B. durch Phishing-Mails, zum Besuch einer bösartigen Website verleitet. Dadurch können Angreifer das Netzwerk nach verwundbaren Multifunktionsdruckern scannen und mittels eines HTTP POST Requests an TCP-Port 9100 einen entsprechend präparierten Druckauftrag an das Gerät senden. Die in dem Dokument enthaltene schadhafte Schriftart ermöglicht es dem Angreifer im Nachgang weiteren Code, wie z.B. einen SOCKS Proxy, auf dem betroffenen Drucker auszuführen [FSE2021b]. Sollte dies einem Angreifer gelingen, könnte er nicht nur sensible Dokumente, die gedruckt, gescannt oder gefaxt werden, sondern auch sensible Informationen wie Zugangsdaten und Passwörter, über die das Gerät mit dem Rest des Netzwerkes verbunden sind, abfließen lassen oder manipulieren. Darüber hinaus kann ggf. weiterer Schadcode auf dem Drucker installiert werden, welcher

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

sich dann wurmartig im Netzwerk ausbreitet, was je nach Netzwerkkonfiguration zu einer kompletten Kompromittierung des Netzwerks führen kann.

Bewertung

Seit mehreren Jahren ist bekannt, dass Netzwerkdrucker teils gravierende Schwachstellen aufweisen. Nicht zuletzt die unzureichenden Antworten der Hersteller darauf machen zusätzliche Maßnahmen auf Anwenderseite erforderlich. Im Gegensatz zu herkömmlichen Komponenten der Infrastruktur, beispielsweise Anwender-PCs oder Server, wird der Sicherheit dieser Geräte jedoch meist nicht genug Beachtung geschenkt. Dies zeigt z.B. die große Zahl von über das Internet erreichbaren Geräten.

Das CERT-Bund des BSI benachrichtigt deutsche Netzbetreiber/Provider täglich zu mehreren hundert offen aus dem Internet erreichbaren IPP-Druckdiensten in ihren Netzen, über die direkt auf die daran angeschlossenen Drucker zugegriffen werden kann. Darunter ist auch eine Vielzahl von HP-Multifunktionsdruckern.

Die Kritikalität eines Druckerangriffs hängt neben dem Schadenpotenzial der in einem Angriff (z.B. Information Disclosure, Code Execution) ausgenutzten Schwachstelle, auch von der jeweiligen Netzwerkumgebung ab. So könnte ein erfolgreich kompromittierter Drucker ggf. auch als Einfallstor und zur Übernahme weiterer Systeme im Netzwerk genutzt werden.

Maßnahmen

Das BSI empfiehlt, die durch den Hersteller zur Verfügung gestellten Sicherheitspatches zeitnah einzuspielen [HEP2021a] & [HEP2021b]. Zudem empfiehlt das BSI, für Drucker einen von Clients und Servern separierten Netzbereich zu verwenden. Dieser Netzbereich sollte von externen Netzen wie dem Internet separiert werden. Da mögliche Angriffe grundsätzlich auch aus dem internen Netz erfolgen können, müssen weitere Sicherheitsmaßnahmen umgesetzt werden. Beispielsweise sollte der administrative Zugang eingeschränkt werden und das Patchmanagement einer Organisation auch die Firmware von Druckern einschließen. Wie Sie Drucker und Multifunktionsgeräte in Ihrem Netzwerk grundsätzlich absichern können, finden Sie auf den folgenden verlinkten Webseiten [ACS2018] & [BSI2020]. Auch HP selbst stellt umfangreiche Best Practices für die Einrichtung von HP Multifunktionsdruckern zur Verfügung [HEP2021c].

Zusätzlich zum Einspielen der Patches, sollten weitere mögliche Maßnahmen zur Sicherung der Multifunktionsdrucker umgesetzt werden:

- Keine grundsätzliche Freigabe von Drucken via USB
- Einrichtung eines eigenen, abgetrennten VLANs mit Firewall
- Einrichtung eines dedizierten Drucker-Servers, über den alle Druckaufträge abgewickelt werden
- Verwendung von Sicherheitsetiketten, um physische Manipulationen an Geräten zu erkennen
- Einsatz von Schlössern (z. B. Kensington-Schlösser), um den Zugriff auf Hardware zu kontrollieren
- Einhaltung der Herstellerempfehlungen zur Verhinderung unbefugter Änderungen an den Sicherheitseinstellungen

Links

[ACS2018] - Drucker und Multifunktionsgeräte im Netzwerk v2.0
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_015.pdf

[BSI2020] - SYS.4.1: Drucker, Kopierer und Multifunktionsgeräte (Edition 2021)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_4_1_Drucker_Kopierer_und_Multifunktionsgeraete_Edition_2021.pdf

[FSE2021a] - PRINTING SHELLZ Bericht von F-Secure
https://labs.f-secure.com/assets/BlogFiles/Printing-Shellz.pdf

[FSE2021b] - PRINTING SHELLZ
https://labs.f-secure.com/publications/printing-shellz

[HEP2021a] - CVE-2021-39237 CVSS-Score 7.1
https://support.hp.com/us-en/document/ish_5000124-5000148-16

[HEP2021b] - CVE-2021-39238 CVSS-Score 9.3
https://support.hp.com/us-en/document/ish_5000383-5000409-16

[HEP2021c] - Technical White paper: HP Printing Security Best Practices for HP FutureSmart Products
http://h10032.www1.hp.com/ctg/Manual/c03137192

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.