Gmail **Ira McDonald <blueroofmusic@gmail.com>**

Security concerns about Print-URI and its use in

3 messages

Kennedy, Smith (Wireless & IPP Standards) <smith.kennedy@hp.com> Thu, May 20, 2021 at 11:43 AM
To: Michael Sweet <msweet@msweet.org>, Ira McDonald <blueroofmusic@gmail.com>

Hi there,

One of my cohorts at HP asked me about a possible security risk involving Print-URI / Send-URI if the printer will willingly try to fetch an arbitrary file over a supported scheme:

- Printer is on a corporate LAN and also on a guest network or has Wi-Fi Direct enabled
- Malicious User connected to printer via Wi-Fi Direct or a guest network
- Malicious User submits a Job using Print-URI or Create-Job / Send-URI, with a URL pointing to a file on a server controlled by the Malicious User
- Malicious User reads server logs to glean information about target printer and the network on which it resides

Has this sort of "vulnerability" been discussed in the past? It seems like Print-URI / Send-URI should be disabled unless a feature / solution depends on it, and also whitelist the domains that can be used?

Smith

/**
Smith Kennedy
HP Inc.
*/

signature.asc
1K

Michael Sweet <msweet@msweet.org> Thu, May 20, 2021 at 11:54 AM
To: "Kennedy, Smith (Wireless & IPP Standards)" <smith.kennedy@hp.com>
Cc: Ira McDonald <blueroofmusic@gmail.com>

Smith,

> On May 20, 2021, at 11:43 AM, Kennedy, Smith (Wireless & IPP Standards) <smith.kennedy@hp.com> wrote:
>
> Hi there,
>
> One of my cohorts at HP asked me about a possible security risk involving Print-URI / Send-URI if the printer will willingly try to fetch an arbitrary file over a supported scheme:
>
> - Printer is on a corporate LAN and also on a guest network or has Wi-Fi Direct enabled
> - Malicious User connected to printer via Wi-Fi Direct or a guest network
> - Malicious User submits a Job using Print-URI or Create-Job / Send-URI, with a URL pointing to a file on a server controlled by the Malicious User
> - Malicious User reads server logs to glean information about target printer and the network on which it resides
>
> Has this sort of "vulnerability" been discussed in the past?

Yes, not only for getting access to content the Client can't directly access, but for a DoS attack (imagine a malicious server that just drips 1 byte per second of a file to keep the printer tied up...)

Unfortunately, we didn't update the security considerations for print-by-reference in STD 92:

> 9.1.3. Print by Reference
>
> When the Document is not stored on the Client, printing can be done by reference. That is, the print request can contain a reference, or pointer, to the Document instead of the actual Document itself -- see Sections 4.2.2 and 4.3.2. Standard methods currently do not exist for remote entities to "assume" the credentials of a Client for forwarding requests to a third party. It is anticipated that print by reference will be used to access "public" Documents. Note that sophisticated methods for authenticating "proxies" are beyond the scope of this IPP/1.1 document. Because Printers typically process Jobs serially, print by reference is not seen as a serious denial-of-service threat to the referenced servers.

:/

> It seems like Print-URI / Send-URI should be disabled unless a feature / solution depends on it, and also whitelist the domains that can be used?

Yes, I've long been an opponent of Print-URI/Send-URI and CUPS has never implemented it. The only time I've ever found it useful is when I wrote the iOS print spooler - when you print a photo we send a user-authorized URI to the photo on the device so we don't have to make an extra copy. Allowing a Client to ask a Printer to grab an arbitrary URL is just asking for trouble IMHO.

____
Michael Sweet

Kennedy, Smith (Wireless & IPP Standards) <smith.kennedy@hp.com> Thu, May 20, 2021 at 1:08 PM
To: Michael Sweet <msweet@msweet.org>
Cc: Ira McDonald <blueroofmusic@gmail.com>

I wonder if we ought to add a "reference-uri-domains-supported (1setOf text(MAX))" that lists domains allowed by the printer...

Smith

[Quoted text hidden]

signature.asc
1K