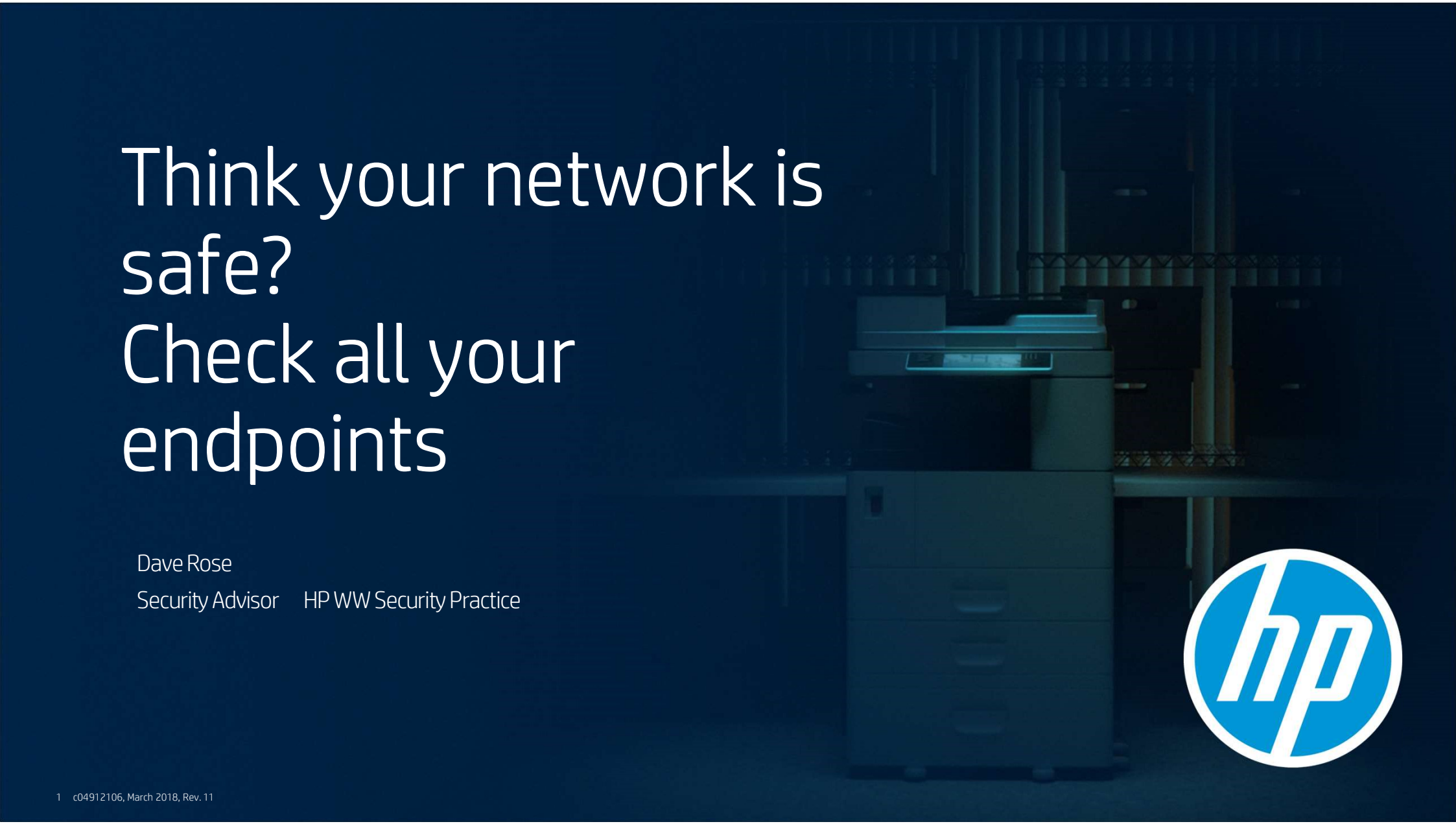
Think your network is safe? Check all your endpoints



Dave Rose

Security Advisor HP WW Security Practice

CHOOSING A DEVICE IS A SECURITY DECISION

Risks of Print… More than fake N

cp<r>
CHECK POINT RESEARCH

PUBLICATIONS TOOLS ABOUT US CONTACT US

Search IPS Protections, Malware Families, Applications and more...

Faxploit: Sending Fax Back to the Dark Ages

Research By: Eyal Itkin and Yaniv Balmas

Fax, the brilliant technology that lifted mankind out the dark ages of mail delivery when
the postal service and carrier pigeons were used to deliver a physical message from a
sender to a receiver.

ITBUSINESSEDGE

Welcome, Guest Log in | Register Like us:

Google Custom Search Search

Home | Slideshows | Blogs | IT Downloads | Research Center | Newsletters | Sponsored Content

IT Management | Data Center | Cloud | Careers | Mobility | Security | Enterprise Apps | Social Media | Big Data | Internet of Things

Home → Blogs → Unfiltered Opinion → Why Fake News On PC And Printer Death Is Dangerous

Related Content

Topic : Network Security
Protect and preserve your network, your data and the life of your business

Blog : Breaches from Third Parties Are the Costliest

Article : What Security Pros Need to Understand About the Dark Web

Why Fake News on PC and Printer Death Is Dangerous

Rob Enderle | UNFILTERED OPINION | POSTED 06 APR, 2017

Share

HP Inc. is the only company with significant positions on both PCs and printers; it dominates the printer market and is ranked second in PCs. Even though it looked like it was initially set up to fail, apparently, the executive staff didn't get that memo **and on most financial metrics, it is growing**. This is in sharp contrast to the beliefs that both PCs and printers are failing. There were two initial causes for this belief. The iPad and similar tablets initially seemed to be a smartphone kind of revolution and were going to take over the world from PCs and printers, and the related drop in support for both categories of products and the massive flip to digital media over print.

However, the primary driver of the PC collapse and the contributing driver of print collapse, tablets, have not risen to expectations. Apple, the lead market maker in the category, has recently flipped from an emerging market strategy to a cash cow strategy with its latest reduced-price iPad offering, suggesting it now believes that tablets are on life support. (Apple is rumored to be working on an iOS-based MacBook.) The HP Inc. results and Apple's latest moves support the counter argument that, while not yet growing at emerging speeds, PCs and printer segments are getting healthier and that strategies based on their expected demise are no longer founded in fact but on fake news. In short, I'm saying that the demise of PCs and printers is effectively no longer true and that making decisions on fake news is dangerous.

Let's get to specifics.

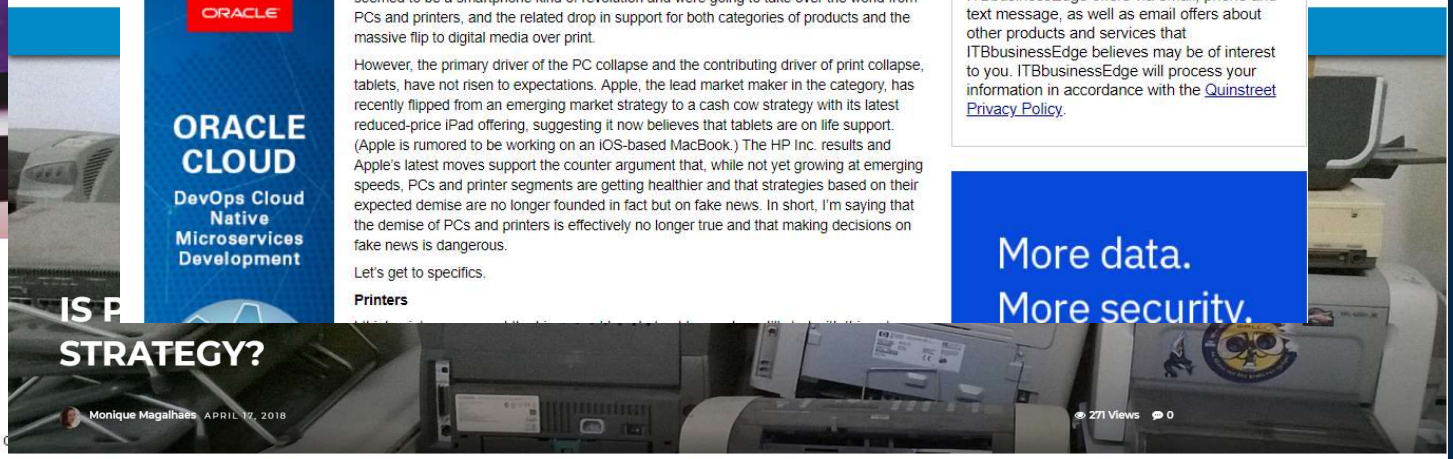
Printers

Subscribe to our Newsletters

Sign up now and get the best business technology insights direct to your inbox.

Enter E-mail Address SUBSCRIBE

By submitting your information, you agree that itbusinessedge.com may send you ITBbusinessEdge offers via email, phone and text message, as well as email offers about other products and services that ITBbusinessEdge believes may be of interest to you. ITBbusinessEdge will process your information in accordance with the Quinstreet Privacy Policy.



SHARE ON FACEBOOK TWEET IT

Your office printers are multifunctional devices that print, scan, fax, copy, scan to cloud, and so on. But

FEATURED PRODUCT

Printer exploited to play Doom on control panel

home
next
previous

Affinity H

home
next
previous

Pri

Print
unive
used

The i
emai

Altho
they
netw

Source: http://abcnews.go

Source: http://www.cbsnews.c

home
next
previous

spy on users, spr
devices to overh

- Printer did not ha
allowed the brea

Source:

Source: http://www.scientificamerican.com/article/printers-can-be-hacked-to-catch-fire/

HP CONFIDENTIAL Internal Use Only

A PRINTER THAT SINGS YOUR DATA FOR HACKERS TO HEAR

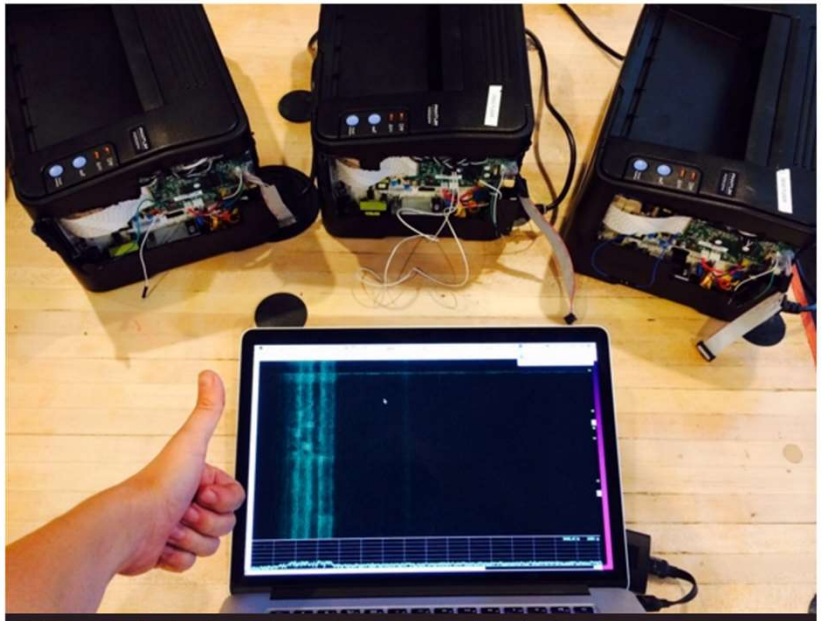
Slate

future tense | THE CITIZEN'S GUIDE TO THE FUTURE | AUG. 5 2015 8:40 AM

A Printer That Sings Your Data for Hackers to Hear

By Lily Hay Newman

40 2



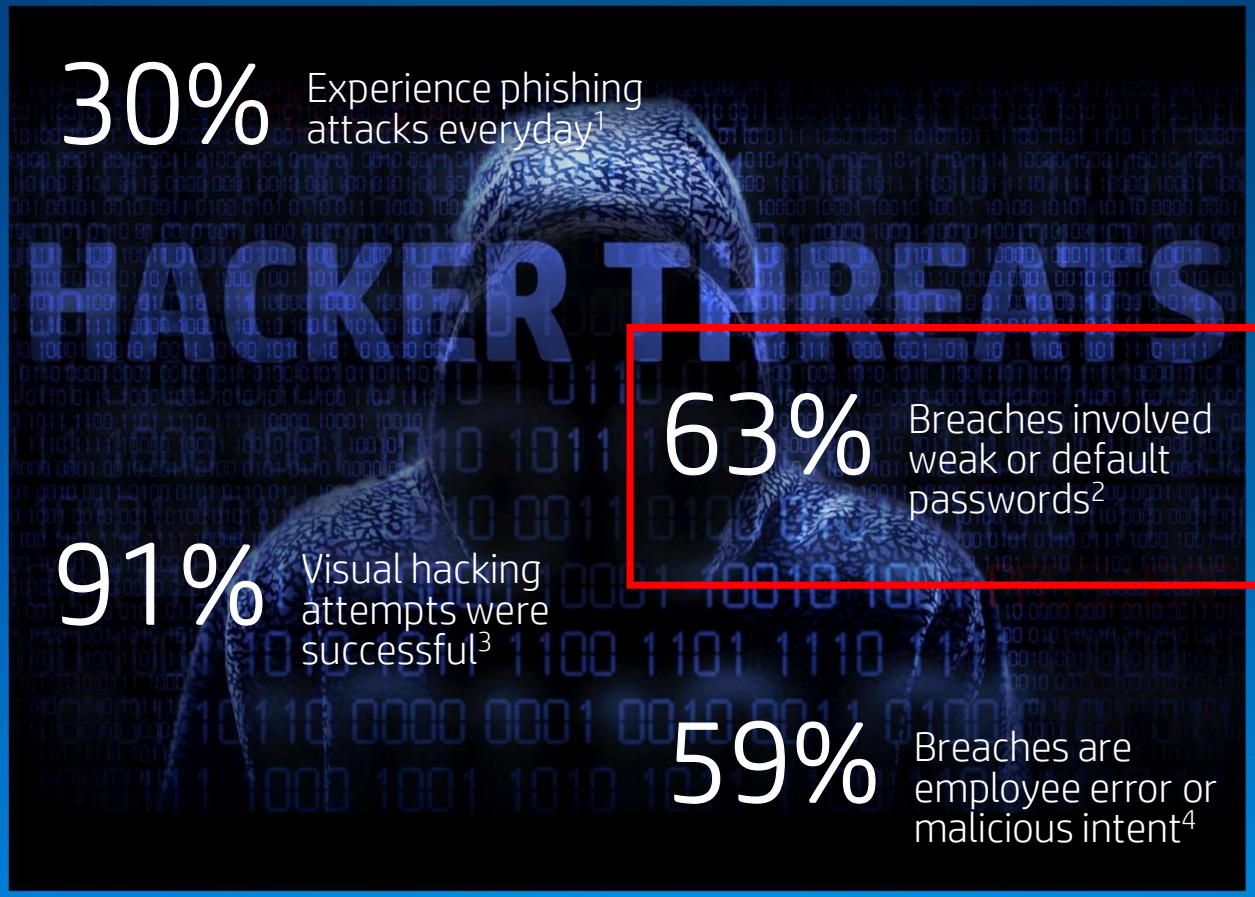
HP CONFIDENTIAL Internal Use Only

Funtenna Video

Go to Youtube and look up funtenna with Motherboard

Some of the Major Overlooked Areas in Printer/Printing Security

Endpoint vulnerabilities



- Malware & viruses
- Device access
- Data flows between devices and network
- Data on hard disks
- Device configuration
- Visual hacking
- Physical loss or theft
- Fraud and counterfeit

[1] 2016 State of Cybersecurity Study, ISACA and RSA Conference, www.isaca.org/state-of-cybersecurity-2016
[2] 2015 Data Breach Investigative Report, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf
[3] 2016 Global Study, http://investors.3m.com/news/press-release-details/2016/New-Global-Study-Reveals-Majority-of-Visual-Hacking-Attempts-Are-Successful/default.aspx
[4] Ponemon Institute, "Global Megatrends in Cybersecurity ," Feb. 2015

The risk is real

It's easy for hackers to break into unsecured printers

"I probe around for a multifunction printer and see that it is configured with default passwords. **Great, I am in…**"

"We've compromised a number of companies using **printers as our initial foothold**. We move laterally from the printer, find Active Directory, query it with an account from the printer and bingo, **we hit GOLD…**"

Peter Kim
Industry-leading penetration Tester, Hacker, Author

Hardware and firmware

Modern malware targets

Software exploit

- Buffer overflow
- Misconfiguration
- Code injection (SQL)
- Open network ports and application vulnerability

Simple physical access exploits

- USB based attack

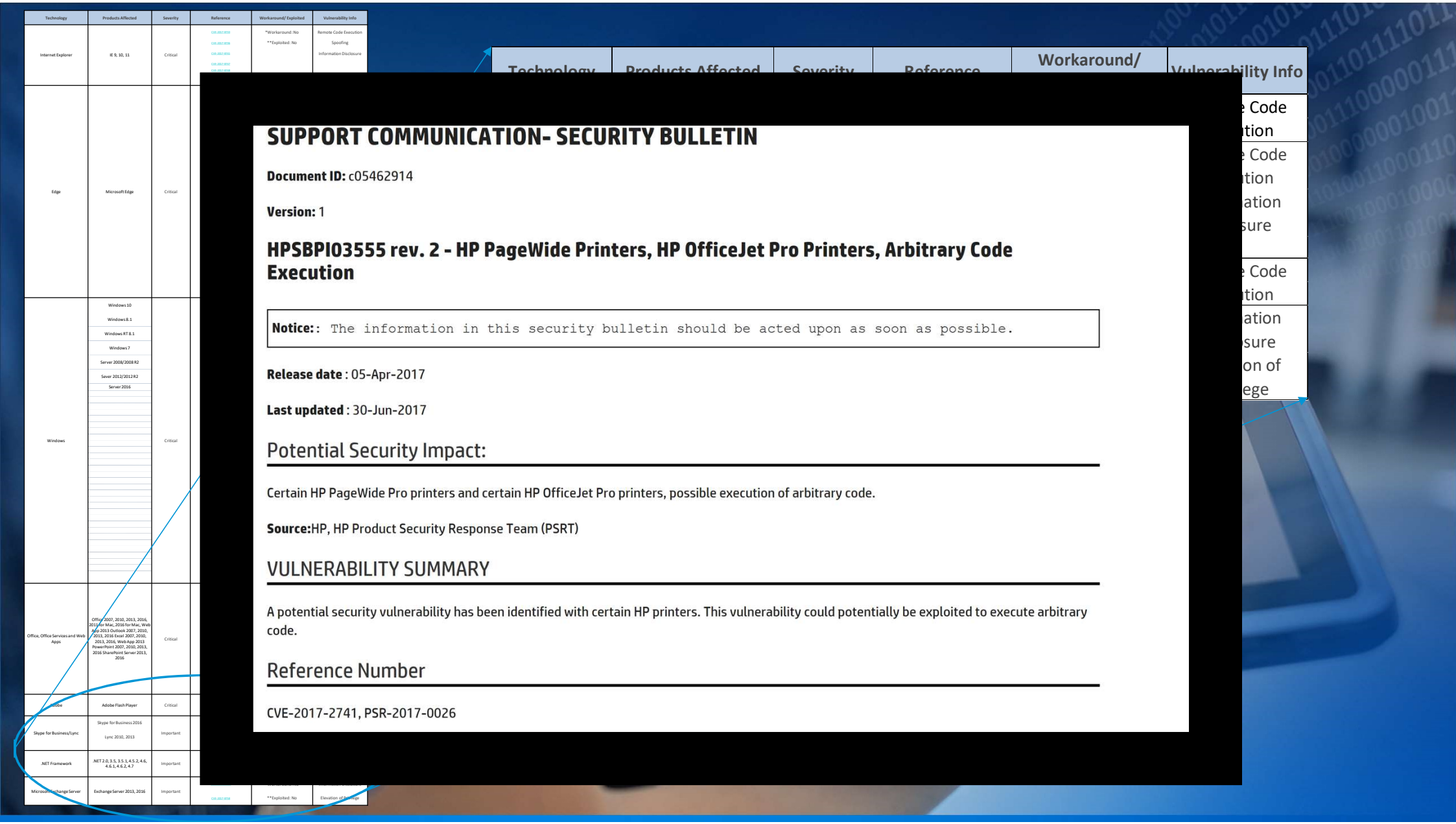
Human exploit

- Phishing email

User space applications

Operating system

Low-level system firmware (UEFI/BIOS)



Technology	Products Affected	Severity	Reference	Workaround/ Exploited	Vulnerability Info
Internet Explorer	IE 9, 10, 11	Critical	CVE-2017-8724 CVE-2017-8736 CVE-2017-8741 CVE-2017-8747 CVE-2017-8748	*Workaround: No **Exploited: No	Remote Code Execution Spoofing Information Disclosure
Edge	Microsoft Edge	Critical			
Windows	Windows 10 Windows 8.1 Windows RT 8.1 Windows 7 Server 2008/2008 R2 Sever 2012/2012 R2 Server 2016	Critical			
Office, Office Services and Web Apps	Office 2007, 2010, 2013, 2016, 2011 for Mac, 2016 for Mac, Web Apps 2013 Outlook 2007, 2010, 2013, 2016 Excel 2007, 2010, 2013, 2016, Web App 2013 PowerPoint 2007, 2010, 2013, 2016 SharePoint Server 2013, 2016	Critical			
Adobe	Adobe Flash Player	Critical			
Skype for Business/Lync	Skype for Business 2016 Lync 2010, 2013	Important			
.NET Framework	.NET 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7	Important			
Microsoft Exchange Server	Exchange Server 2013, 2016	Important	CVE-2017-8758	**Exploited: No	Elevation of Privilege

SUPPORT COMMUNICATION- SECURITY BULLETIN

Document ID: c05462914

Version: 1

HPSBPI03555 rev. 2 - HP PageWide Printers, HP OfficeJet Pro Printers, Arbitrary Code Execution

Notice:: The information in this security bulletin should be acted upon as soon as possible.

Release date : 05-Apr-2017

Last updated : 30-Jun-2017

Potential Security Impact:

Certain HP PageWide Pro printers and certain HP OfficeJet Pro printers, possible execution of arbitrary code.

Source:HP, HP Product Security Response Team (PSRT)

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with certain HP printers. This vulnerability could potentially be exploited to execute arbitrary code.

Reference Number

CVE-2017-2741, PSR-2017-0026

Cybersecurity Framework Inclusion Of Endpoints


JUSTICE
IS
COMING

NISTIR 8023

Risk Management for Replication Devices

Kelley Dempsey
Celia Paulsen

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8023

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Security Risk Assessment Table for Replication Devices (RDs)

Replication Device Information

Manufacturer and Model:

Associated System ID:

Assessment Information

Date of Assessment:

Name(s) of Assessor(s):

#	Risk-Related Question	Yes, No, or N/A	Risk Score	Accept Risk? (Y/N)*	Action** or Justification for Risk Acceptance
	PLANNING/SECURE CONFIGURATION				
1	Is the device included within a system security plan with applicable controls implemented?		(Yes=0; No=4)		
2	Does the device or its control software have any relevant security certifications (e.g., Common Criteria)?		(Yes=0; No=1)		
3	Does the vendor/manufacturer provide information on a secure configuration for the device?		(Yes=0; No=1)		
3.1	If a secure configuration is available, has it been implemented on the device?		(Yes=0; No=2)		
	THIRD PARTIES				
4	Is the device leased by the organization? (N/A if the organization owns the device)		(Yes=3; No=0)		
4.1	If leased, does the lease agreement stipulate federal ownership of storage devices internal to the device? (N/A if the organization owns the device)		(Yes=0; No=4)		
5	Is the device under a service contract?		(Yes=0; no=2)		
5.1	If under service contract, does the service contract stipulate that hard disk drives (HDDs) and solid state/nonvolatile storage must be removed before the device can leave		(Yes=0; no=5)		

Building trust with device security

Design for cyber-resilience

Protect

Detect

Recover

Software security is **not enough**
Must start from the **firmware up**

Secure the Device

HP Sure Start

Keeps the BIOS safe and self-heals

Whitelisting

Keeps the firmware safe

Run-time intrusion detection

Monitors run-time operations and self-heals

HP Connection Inspector

Monitors network connections and self-heals

HP Security Manager

Checks and remediates printer settings

HP JetAdvantage Security Manager

Comprehensive security management with policy-based print security compliance

HP Security Manager makes it easy to monitor and protect your entire fleet:

- **Strengthen compliance** to corporate security policies
- **Streamline security management** by automating many processes
- Get efficient fleet management of **device certificates**
- **Secure new devices immediately** with Instant-on Security

HP Quick Assess (with JetAdvantage Security Manager)

Demonstration that assesses the top 13 security settings on up to 20 HP printers

HP JetAdvantage Security Manager
Device Assessed Details Report

Report run at 9/23/2015 11:41:14 AM — Page 1 of 1

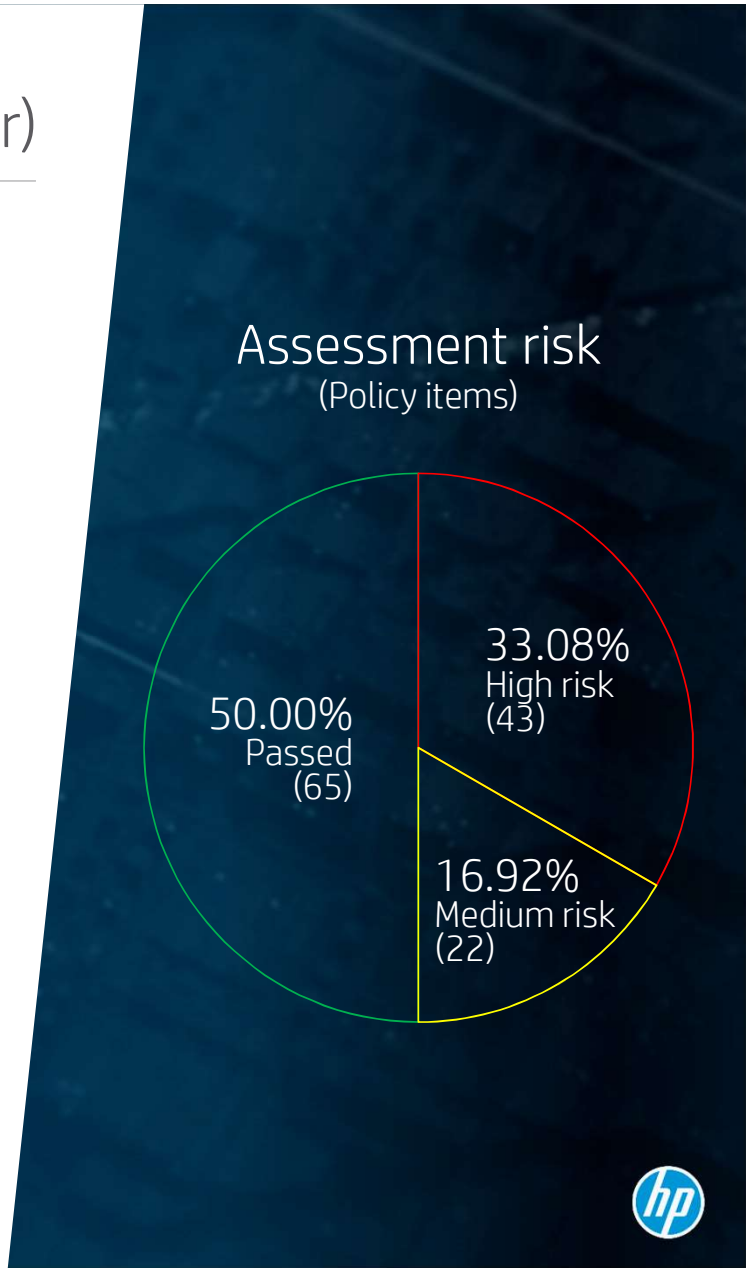
Device: HP Officejet Color FlowMFP X585 (15.25.214.189) — Risk: High, Medium, Low, Pass

Policy: Limited	Date Run: 9/21/2015 1:23:55 PM
Device Control	
File System Access Protocols	
Allow PS Access	Value Mismatch {Policy: Disabled, Device: Enabled}
Allow PJL Access	Value Mismatch {Policy: Disabled, Device: Enabled}
Network Services : Web	
Require HTTPS Redirect	Passed
Authentication : Credentials	
PJL Password	Password Not Set
SNMPv3	Value Mismatch {Policy: Enabled, Device: Disabled}
SNMPv3 Credentials	Credentials Not Set
SNMPv1/v2	Value Mismatch {Policy: Read Only Enabled, Device: Read and Write Enabled}
Read Community Name	Password Not Set
Read/Write Community Name	Password Not Set
Admin (EWS) Password	Passed
File System Password	Passed
Printing	
File Transfer Protocol (FTP)	Value Mismatch {Policy: Disabled, Device: Enabled}
AppleTalk	Passed
Novell (IPX/SPX)	Passed
Network Services	
Telnet	Value Mismatch {Policy: Disabled, Device: Enabled}
Remote Firmware Upgrade (RFU)	Value Mismatch {Policy: Disabled, Device: Enabled}
FTP Firmware Update	Passed

This report is provided for general comparison only. The information contained is based on manufacturer's published and internal specifications, and proprietary data and algorithms. The information is not guaranteed accurate by HP Development Company. Users can customize the security policies used in the analysis, which will affect the results. Actual results may vary.

Unconfirmed passwords/ certificates could lead to unauthorized access to the device

Unused protocols left unsecure could become an entry point onto the network



TAKE ACTION NOW

Getting started

Engage your Sales Representative

Bring in the experts

Run an assessment

Know your risks

Develop a plan

Secure your print fleet

THANK YOU

David Rose

David.rose3@hp.com

813-731-0300