Configuring Security Mitigation Settings for Security Bulletin HPSBPI03569



Protecting Solution Installation Settings

Table of contents

Overview	2
Using the Embedded Web Server (EWS)	2
Set the local administrator password	2
Disable "Allow firmware updates sent as print jobs (port 9100)"	4
Using HP Web Jetadmin to configure multiple devices	6
Discovering devices in Web Jetadmin	6
Creating and Adding Devices to a Web Jetadmin Group1	1
Creating a Web Jetadmin template for Security Migration Settings	3
Applying the Web Jetadmin template for Security Migration Settings	6

Overview

This document provides instructions for mitigation steps you can take to prevent exposure to the remote code execution vulnerability (CVE-2017-2750). These instructions apply to HP Enterprise printers and multi-function printers running FutureSmart version 3 and FutureSmart version 4. Configure the following two settings:

- Set the Local Administrator password for the Embedded Web Server (EWS). A password must be configured before access to the Solution Installer is permitted.
- Disable the "Allow firmware updates sent as print jobs (Port 9100)" setting in the EWS. This prevents solution packages from being uploaded through the firmware update method.

Using the Embedded Web Server (EWS)

Set the local administrator password

To allow access to the Solution Installer, follow the steps below to set the local administrator password for the Embedded Web Server (EWS).

1. Open a web browser and enter the printer IP Address or host name in the browser address field. If you do not know what the IP Address or host name is, ask your administrator.

Figure 1: Entering the IP Address



NOTE:

If a certificate warning appears, proceed to the printer EWS. A certificate warning is normal if the printer is using a self-signed certificate.

2. Select the Security tab. By default, General Security will be selected in the left panel.

Figure 2: Selecting the Security tab in the EWS

(p)	HP 15,41,190,162			Security Security
Inform	ation General Security and	Fax	Supplies	Troubleshooting Security HP Web security
Ceneral S	General Security			Нер

NOTE:

If a password is required, click the Sign In button, sign in, and then skip the next two steps.

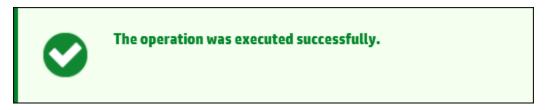
3. In the **Set the Local Administrator Password** section of **General Security**, set the local administrator password in the **New Password** and **Verify Password** fields.

Figure 3: Setting the password

Set the Local Administrator Password	an a she shi yani ni ba sa sana na ay il san	ale per de cue cancelar per la cancelar de cancelar de cancelar de cancelar de ca
		emotely configuring the device or gaining access to functionality is also the Device Administrator Access Code at the device.
User Name		
admin		
Old Password	New Password	Verify Password
Password is not set.		

4. Click the **Apply** button in the bottom right area of the EWS. If successful, a confirmation message appears at the top of the page.

Figure 4: The success message



Print devices running FuturesSmart 4 require a complex password with a minimum of eight characters, and must contain a combination of three of the following: uppercase letters, lowercase letters, numbers, and special characters. Otherwise, a failure message will appear.

Figure 5: The password reset failure message



The operation has failed.

Please correct the errors below and try again.

 The password must contain three of the following: upper case letters, lowercase letters, numbers, and special characters. 5. To change password complexity requirements, click **Account Policy** in the left panel and update the fields under **Local Administrator Password**.

Account Policy		Help
Local Administrator Password		
Enable account lockout		
Maximum attempts	Lockout interval	Reset lockout counter interval
5	10	10
(3-30)	(5-1800) seconds	(0-1800) seconds
Enable password complexity When checked, the password must Minimum password length	contain three of the following: uppercase letters	s, lowercase letters, numbers, and special characters.
0		
Zero (0) indicates that the minimur	m password length is disabled; no password is re-	quired.
		Apply Cance

Figure 6: Changing password complexity requirements

Disable "Allow firmware updates sent as print jobs (port 9100)"

1. Open a web browser and enter the printer IP Address or host name in the browser address field. If you do not know what the IP Address or host name is, ask your administrator.

NOTE:

If a certificate warning appears, proceed to the printer EWS. A certificate warning is normal if the printer is using a self-signed certificate.

- 2. Select the Security tab. By default, General Security will be selected in the left panel.
- 3. In the **Firmware Upgrade Security** section of General Security, uncheck **Allow firmware updates sent as print jobs (port 9100)**. This also prevents sending print solution and device firmware over certain paths.

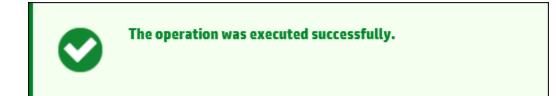
Figure 7: Disabling firmware upgrades sent as print jobs

Firmware Upgrade Security
Allow firmware upgrades sent as print jobs (port 9100)

4. Click the **Apply** button in the bottom right area of the EWS.

If successful, a confirmation message appears at the top of the page.

Figure 8: The success message



Using HP Web Jetadmin to configure multiple devices

HP's Web Jetadmin fleet management tool can be used to set the two remediation settings simultaneously across multiple devices. The HP Web Jetadmin software is a free tool and is available for download at www.hp.com/go/webjetadmin.

HP Web Jetadmin can be installed on a single workstation or can be installed as a client-server application in an enterprise environment.

Discovering devices in Web Jetadmin

1. In the **Device Management** navigation panel, right-click **Discovery**, and then select **Discover devices**.

Figure 9: Launching the Device Discovery wizard

🛷 HP Web Jetadmin - localhost	
File View Tools Help	
Device Management	🖻 Discovery
Overview All Devices (0) Error Devices (0) Warning Devices (0) Warning Devices (0) Warning Devices (0) Warning Devices (0) Ungrouped Devices (0) Groups Discover devices Discover devices Discover devices Discover devices Create discovery template Sto Sto Delete discovery template Copy discovery template View discovery history.	e e late ste

The Device Discovery wizard starts.

2. Select the Network connected devices option.

3. Select the **IP range** check box and click the **Next** button.

Figure 10: Specifying discovery options

Device Discovery	?	\times
Specify discovery options		ĺ
Discovery options		
O Use template:		
<no templates=""></no>		
Specify settings:		
Network connected devices		
SLP multicast		
17 breadcast		
☑ IP range		
Specified addresses		
Active Directory		
WS-Discovery		
O PC connected devices		
IP broadcast		
IP range		
Specified addresses		
Active Directory		
Domain		
WS-Discovery		
Schedule discovery		-
	Next > Can	cel

4. Click the **Add** button in the **Select IP ranges** dialog.

5. In the Add IP Range panel, enter a starting and ending IP range in the **First address** and **Last address** fields, and then click the **Add** button.

Figure 11: Adding	the IP	address	range
-------------------	--------	---------	-------

🐔 Add IP Range						\times
First address:						
Last address:						
Description:						
Calculate range	<u>e</u>					
		_				
			.Add		Clos	se

- 6. Click the **Close** button on the **Add IP Range** panel, then click the **Next** button.
- 7. If a SNMPv1 get community name is configured for print devices, select **Specify** credentials.

8. Select the **SNMPv1 Get Community Name** checkbox, enter the get community name in the field, and then click **Next**.

Specify credentials	a .
))
O De not use credentials	
Specify credentials to use for this discovery SNMPv1 Get Community Name	
SNMPv1 Get Community Name	
Global credoctials	
Use global credentials	
< Back Next Cance	ł

Figure 12: Entering the Get Community Name

9. Select **Start** to begin device discovery.

10. Click the **Details** button in the lower-left area to view discovered devices.

Figure 13: Viewing details for discovered device
--

Device Discovery		?	×
Results			_
Discovery complete			
Overall status			
Elapsed time (hh:mm:ss):	00:00:14		
Started by:	In the second		
Progress (estimated):	100%		
Node discovery			
Current method:	Node discovery complete		
Nodes found:	1 nodes found		
Device resolution			
Nodes resolved:	1 of 1 nodes resolved		
Devices found (this discovery):	1		
New devices (this discovery):	1		
View all devices			
Details		D)one

11. Close the **Discover Results** dialog and click the **Done** button.

Creating and Adding Devices to a Web Jetadmin Group

1. In the **Device Management** navigation panel, right-click **Groups**, and then select **New Group**.

Figure 14: Creating a new group

🦪 HP I	Neb Jeta	admin - Io	ocalhost								
File	View	Tools	Help								
Devi	ce Ma	nagen	nent		R	All D)evices	i (0 e	of 1 Selec	ted)	
	Dverviev	-	•		关				Layouts 👻 🔤	🝸 Filters	- 🕄
±		evices (1) ns				Devi	çe Model		IP Address	IP Hostna	ame
	ě 🚬	Scarch) — i —	1 .]	643,70402	i prode UK	u.h
	<u>کم ک</u>	New gr	qup								
		Edit gro	up	/			I				
		Add de	vices to	group			I				
€.(Remov	e devices	from gr	oup		I				
±.∜	3	Delete g	group				I				
	2	Edit gro	oup polic	ies			I				
		Import	groups				I				
		Export	groups								
		Expand	all				1				
		Collaps	e all				I				
	_										

The Create Group wizard starts.

- 2. Enter RCE Security Template in the Group Name field.
- 3. Select the **Configure group properties now** checkbox, then click the **Next** button.
- 4. Press the CTRL plus A buttons to select all of the devices in the **Available devices** panel.

5. To add the devices to the **Devices in group** list, click the double-arrow >> button, and then click the **Next** button.

	Group					?	Ē
elect	devices						
	devices All Devic			Devices in group Number of device	s: 0		
Device I	Luciation	IP Hostname	IP Address	Device Model	IP Hostname	IP Address	1
	J.						
				66.2			
					< Back Next	Can	

Figure 15: Selecting devices

- 6. Enter a group description, then click the **Next** button.
- 7. Click the **Next** button in the **Configure Group Policies** dialog.

8. Click the **Create Group** button in the **Confirm** dialog, then select **Done**.

Figure 16: Creating a group

Confirm Settings Group name: RCE Set Devices	
Group name: RCE Set Devices	
Parent group: <no parent=""></no>	
Description: <not specified=""></not>	
Contact: <not specified=""></not>	
Membership type: Manual (0 devices)	
Policies: 0	
< Back Create Grup Can	cel

Creating a Web Jetadmin template for Security Migration Settings

1. In the **Device Management** navigation panel, click the plus sign
→ next to **Configuration** to expand the menu.

2. Right-click **Templates** and select **Create configuration template**.

File View Tools Help	
Device Management	Configuration Templates
Overview All Devices (1) Groups Discovery	Control Panel Display (Default) Printer Wakeup (Default)
Configuration History Aler Firm Rep Stor Solu Create configuration Create configuration Edit configuration te Delete configuration te Copy configuration te Export configuration te	template mplate template template
Import configuration	

Figure 17: Creating the configuration template

3. In the **Select Template Models** dialog, select the desired printing device models or use the **Search** field to locate specific printer models.

4. To add models to the **Selected** list, click the model name in the **Available** list, click the double-arrow >> button, and then click **Next**.

Create Device	e Configuration Template		?	>
elect Temp	blate Models		-	1
Devices Available Search Model Name		Selected Number of models: 0 Model Name		
Network Cards Available		Selected		

Figure 18: Adding devices

- 5. Enter RCE Security Template in the Template Name field.
- 6. In the **Device Settings** list, click the plus sign 🗉 next to **Security** to expand the list.
- 7. Select the **Embedded Web Server Password** setting, and enter a password in the **Password** and **Confirm Password** fields.
- 8. Select the **Printer Firmware Update** setting, and select the **Disable** radio button.

9. Click the **Next** button.

pecify template options					4
Template name Name:					
Device settings					
My Settings Device Wireless Supplies Copier Fax Security Access Control for Device Bootloader Password Device User Accounts Digital Sending Service Disable Direct Ports Display Options on Inform Embedded Web Server P Enable Host USB plug an Enable Host USB plug an Enable PJL Device Acces EWS Information Protecti LDAP Sign In Setup LDAP Users and Groups Near Field Communication PJL Password Printer Firmware SHA1 C Printer Firmware Update Restrict Color Secure Disk Password Secure Disk Password Secure Disk Password	×	inter Firmwa Disable Enable	e		2

Figure 19: Disabling Printer Firmware Update

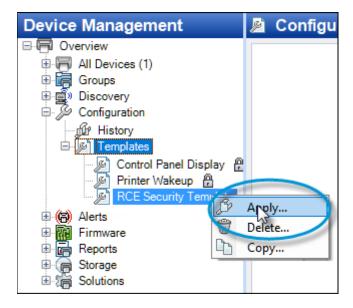
10. Select **Create Template**, then click **Done**.

Applying the Web Jetadmin template for Security Migration Settings

- 1. In the **Device Management** navigation panel, click the plus sign next to **Configuration** to expand the menu.
- 2. Expand the **Templates** menu.

3. Right-click the **RCE Security Template** and select **Apply**.

Figure 20: Applying the RCE Security Template



- 4. In the **Specify configuration options** dialog, click the **Next** button.
- 5. Select the **Groups** radio button in the **Select devices** dialog.

6. Select **RCE Settings Devices** from the **Group** drop-down list, then click the **Next** button.

Figure 21: Selecting groups

Apply Device Configuration Template	?	×
Select devices		Ş
Selection method O Devices Groups		
Selected group Group: RCE Settings Devices		
< Back Next	Ca	ncel

- 7. Click Apply Template.
- 8. Review the **Results** dialog to confirm the template settings were applied successfully.

9. Click the **Details** button to review the results or address any errors.

Figure 22: Reviewing the Device Configuration Results

Apply Device Configuration Template			×
Results			Þ
Success			
Summary Success:	1		
🛓 Warning:	0		
😳 Error:	0		
i Information needed:	0		
Pending:	0		
Details		Do	one

© Copyright 2018 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.