

Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	1 of 10
Action Required:	Information Only				

## How to Upgrade Firmware to Guard Against Potential Vulnerabilities

#### Summary

A command injection vulnerability in the web server of some Hikvision products has been identified. In the case of insufficient input validation, an attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.

First, identify the products affected by the vulnerability, then find that product's specific updated firmware using the following link:

Security Notification- Command Injection Vulnerability in Some Hikvision products | Hikvision Canada | The world's largest video surveillance manufacturer

#### Note: Please do not power off any device during the upgrade process.

Hikvision offers multiple ways to upgrade firmware. Users can choose from among five upgrade methods according to the device type and/or preference.

Please continue reading and select the appropriate method for your application(s).



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	2 of 10
Action Required:	Information Only				

#### Method 1: Batch Upgrade (NVR, IPC, & PTZ products)

First, please download the Batch Configuration Tool at this link:

https://ca.hikvision.com/en/support-resources/downloads/tools

- 1. After downloading and opening the software, click on the devices requiring the upgrade
- 2. Then click on "+Add"
- 3. Enter the User Name and Password
- 4. Then click "OK"

Tota	al Numbe	er: 10   💭	Refresh	+ Add	imes Delete	📴 Upgrading D	letection 🖵 Upgrade	e 🚯 Export Upgrade R	eport	Î.		Fil	ter		
				💷 Heal	th Monitoring	🕒 Export Device	Set bbA	System Configuration	•	⊙ N	lore 👻				
	ID	Device Type	iP Addre	ess Port	Channel	Firmware Version	Serial No.	Upgrade	Operatio	n		Status			
	000005	iDS-2PT9122IX-DI	E/S 192.168.	250.106 8000		V5.4,9 build 171207	iDS-2PT9122IX-DE/S201	Unknown	0 5	۵	0	Online			
	000006	DS-2TD1217B-3/P	PA 192,168.	250.95 800		V5.5.26 build 200904	DS-2TD1217B-3/PA2020	Unknown	(2)	0	0	Online			
	000007	DS-2DF8836/V-AE	LW 192.168.	250.126 8000		V5.4.71 build 170309	DS+2DF8836/V+AELW201	Unknown	0 9	۲	•	Online			
	800000	DS-2PT3326IZ-DE	. J	-			DS-2PT3326IZ-DE320170	Unknown	0 9	•	0	Online			
	000009	DS-2TD1217-2/V1	Us 15	ser Name ad	lmîn	3	DS-2TD1217-2/V1202004.,	. Unknown	0 6	Þ	0	Online			
	000010	DS-2DE4A425IW-	DE 11 F	Password		1	DS-2DE4A425IW-DE2018.	. Unknown	0 7	0	0	Online			
	50		2		4	ОК						< >		1	1
	50 Numbe			Add 🗘 /	4	Reset Password	Edit Network Parameters	🔅 One-Touch Apply	() On	e-Touc	< h Config			1	/1
ota	l Numbe			Add		1000 million (1000 million)	Edit Network Parameters IPv4 Gateway: HTTP F		-	e-Touc	h Config		ter	1	
Tota	l Numbe	n 59 📿 Ref	iresh +		-   Port	Reset Password			Sub		h Config sk	ure O Fi	ter ss	1 Encodin 0	
Tota	ID I	r: 59 📿 Ref Device Type	Fresh + i	IPv4 Address	-   Port	Reset Password	IPv4 Gateway HTTP F	Port Device Serial No.	Sub	net Ma 255.25	h Config sk l	MAC Addre	tor ss 5-4c-d6		
Tota	ID I	n 59 📿 Ref Device Type IDS-9632NXI-18/165	Security Activated	IPv4 Address	Port	Reset Password Firmware Version V4.1.25build 181028	IPv4 Gateway   HTTP F 192.168.250.1 80	Port Device Serial No. iDS-9632NXI-I8/165162	Sub 0 255 1 255	net Ma 255.25 255.25	h Config sk   5.0	ure <b>o</b> Fi MAC Addre 18-68-cb-al	tor 55 5-4c-d6 6-4c-2e	0	
	I Numbe ID   047 058 048	n: 59 🏾 🎘 Ref Device Type iDS-9632NXI-18/165 DS-96256NI-124/H	Security Activated Activated	IPv4 Address 192.168.250.3 192.168.250.3	Port   10 8000 11 8000 12 8000	Reset Password Firmware Version V4.1.25build 181028 V4.40.506build 201218	IPv4 Gateway HTTP F 192.168.250.1 80 192.168.250.1 80	Port Device Serial No. iDS-9632NXI-18/165162 DS-96256NI-124/H3220	Sub 0 255 1 255 0 255	net Ma 255.25 255.25 255.25	h Config sk   5.0 5.0	MAC Addre 18-68-cb-ai 54-c4-15-el	tor 5-4c-d6 1-4f-52	0	
	I Numbe ID   047 058 048	r: 59 $\bigcirc$ Ref Device Type IDS-9632NXI-I8/165 DS-96256NI-I24/H BIAZEF PT0/ (28/10H	Activated Activated Activated	IPv4 Address 192.168.250. 192.168.250. 197.168.250.	- Port 10 8000 11 8000 12 8000 13 8000	Reset Password Firmware Version V4.1.25build 181028 V4.40.506build 201218 V4.1.62build 181019	IPv4 Gateway         I HTTP F           192.168.250.1         80           192.168.250.1         80           192.168.250.1         80	Port Device Serial No. iDS-9632NXi-18/165162 DS-96256NI-124/H3220 Blazer Pro/128/16H322	Sub 0 255 1 255 0 255 2 255	net Ma 255.25 255.25 255.25	h Config sk   5.0 5.0 5.0	MAC Addre 18-68-cb-ai 54-c4-15-ei b4-a3-82-d	tor 5-4c-d6 6-4c-2e 1-4f-52 9-e4-16	0 0 0	/11
	I Numbe ID   047 058 058 051	r: 59 $\bigcirc$ Ref Device Type DS-9632NXI-18/165 DS-9632NXI-18/165 DS-96256NI-124/H BIATER PRO-125/164 105-9632NXI-18/X(B)	Security Activated Activated Activated Activated	<ul> <li>IPv4 Address</li> <li>192.168.250.3</li> <li>192.168.250.3</li> <li>190.168.250.3</li> <li>190.168.250.3</li> </ul>	Port           0         8000           11         8000           12         8000           13         8000           14         8000	Reset Password Firmware Version V4.1.25build 181028 V4.40.506build 201218 V4.1.62build 181019 V4.22.110build 200609	IPv4 Gateway         I HTTP P           192.168.250.1         80           192.168.250.1         80           192.168.250.1         80           192.168.250.1         80	Device Serial No.           iDS-9632hXi-I8/165162           DS-96256NI-I24/143220           Blazer Pro/128/16H322           iDS-9632hXi-I8/X(B)16	Sub 0 255 1 255 0 255 2 255	net Ma 255.25 255.25 255.25 255.25	h Config sk   5.0 5.0 5.0 5.0	MAC Addre 18-68-cb-a/ 54-c4-15-el b4-s3-82-d ac-cb-51-ci	ter 5-4c-d6 5-4c-2e 1-4f-52 5-e4-16 1-c8-ae	0 0 0	

- 5. Search for the device on Hikvision's official website link also provided above: Fix Firmware Download Index
- 6. Click on "Download" to download the firmware
- 7. After downloading the firmware, select the device requiring the upgrade
- 8. Then click on "Upgrade"

5	Batch G	onfiguration								û 🕸 û	_ 🗆 ×
Total	Number: 1	10   C Refi	resh + Ad	d )	× Delete	🔯 Upgrading D	etection	🗟 Export Up	grade Report	Filter	
		🔂 Bate	ch Copy 🚥	Health	Monitoring	Export Device	G Add IPC	<li>System Confi</li>	guration 💌 💮 More 💌		
10	o i	Device Type 🍸 🛛	IP Address	Port	Channel	Firmware Version	Serial No.	Upgrade	Operation	Status	
□ 0	00005	iDS-2PT9122IX-DE/S	192.168.250.106	8000		V5.4.9 build 171207	iDS-2PT9122IX-DE/S201	Unknown	\$ F 0 <b>(</b>	Online	
0	00006	DS-2TD1217B-3/PA	192.168.250.95	8000		V5.5.26 build 200904	DS-2TD1217B-3/PA2020	Unknown	\$ F © <b>(</b>	Online	
0	00007	DS-2DF8836IV-AELW	192.168.250.126	8000		V5.4.71 build 170309	DS-2DF8836IV-AELW201	Unknown	\$ F © <b>(</b>	Online	
7 0	80000	DS-2PT3326IZ-DE3	192.168.250.124	8000		V5.4.12 build 180530	DS-2PT3326IZ-DE320170	Unknown	\$	Online	
0	00009	DS-2TD1217-2/V1	192.168.250.230	8001		V5.5.22 build 210619	DS-2TD1217-2/V1202004	Unknown	\$ <b>4 6</b>	Online	
0	00010	DS-2DE4A425IW-DE	92.168.250.134	8000		V5.6.15 build 191211	DS-2DE4A425IW-DE2018	Unknown	\$₽ €	Online	

© 2021 Hikvision Canada Inc. All Rights Reserved. 2355 Skymark Ave, Suite 300, Mississauga, ON L4W 4Y6 • Phone: +1 866-200-6690 E-Mail: <u>techsupport.ca@hikvision.com</u> • www.hikvision.ca



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	3 of 10
Action Required:	Information Only				

- 9. Select "File Upgrade"
- 10. Click on the file path
- 11. Select the Digicap.dav file
- 12. Click on "Open"
- 13. Then click "Ok" to start the upgrade process

9 Upgrading Mode • File Upgrade File Path daniel.garay/Desktop		grade O Local Upgrade	
5 Open			×
← → × ↑ 📙 « Firmwares → kc001	5 V	Search kc001	P
Organize - New folder		BEE - 07	1 0
Daniel CCTV	í.	Date modified	Typ
employee forms digicap.dav		7/14/2020 12:14 PM	DAV
hik connect		17 19 2020 12:14 P.W	UN
This PC 3D Objects			
Desktop			
Documents			
➡ Downloads			
10.00 g			
File name: digicap.dav	4.0		~
	12	Open Can	cel

U	pgrade Pro	ogress 🤇		100%			Upgrade completed.	Total: 1 S	ucceeded: 1 Failed: 0	
. 1	ID	Device Type	IP Address	Port	Channel	Firmware Version	Serial No.	Upgrade	Operation	Status
0	000001	DS-2CD7126G0/L-IZS	192,168.250,103	8000		V5.5.81 build 180910	DS-2CD7126G0/L-IZS20	Unknown	# F • •	Online
	000002	DS-2CD7526G0-IZHS	192.168.250.127	8000		V5.6.0 build 190428	DS-2CD7526G0-IZHS201	Unknown		Online
1	000003	PCI-LB15F2SL	192,168,250,117	8000		V5.5.160 build 210416	PCI-LB15F2SL20201119A	Unknown	\$ \$ D	Online
	000004	PTZ-N5225I-AE	192,168,250,119	8000		V5.5.3 build 180211	PTZ-N5225I-AE20170929	Unknown	\$ 4 D	Online
1	000005	iDS-2PT9122IX-DE/S	192.168.250.106	8000		V5.4.9 build 171207	iDS-2PT9122IX-DE/S201	Unknown		Online
8.	000006	DS-2TD1217B-3/PA	192.168.250.95	8000		V5.5.26 build 200904	DS-2TD1217B-3/PA2020	Upgrade completed.		Online
1	000007	DS-2DF8836IV-AELW	192,168.250.126	8000		V5.4.71 build 170309	DS-2DF8836IV-AELW201	Unknown	\$	Online
	800000	DS-2PT3326IZ-DE3	192.168.250.124	8000		V5.4.12 build 180530	DS-2PT3326IZ-DE320170	Unknown	\$ 7 D <b>(</b>	Online
0	000009	DS-2TD1217-2/V1	192,168,250,230	8001		V5.5.22 build 210619	DS-2TD1217-2/V1202004	Unknown	@ <del>-</del> • •	Online
	000010	DS-2DE4A425IW-DE	192.168.250.134	8000		V5.6.15 build 191211	DS-2DE4A425IW-DE2018	Unknown	\$ G 0	Online



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	4 of 10
Action Required:	Information Only				

### Method 2: Upgrade via Web Interface (NVR, IPC, & PTZ products)

<b>(</b>	2	3/doc/page/config.asp	4	ID address to la	n in the cost	▼ Ů 搜索		۰ م	\$\$ \$\$ \$\$
Orr	figuration	× 🖸 🔰 S	tep 1: input the	IP address to lo	g in the web	interace.			
		Live View Playb	ack Picture	Configuration			👤 admin	👔 Help	🗗 Logout
Q	Local	Upgrade & Maintenance	Online Upgrade Log	Diagnose Step 2:	Click 'Configu	uration'			
	System	Reboot							
	System Settings	Reboot	Reboot the device.						
	Maintenance	Default							
Step	Security 3: Click 'Main Camera Management	tenance <sup>kestore</sup>	Reset all the parameters, e	xcept the IP parameters and us	er information, to the defa	ault settings.			
	User Management	Default	Restore all parameters to c	efault settings.					
Ð	Network	Export							
<u>Q.</u>	Video/Audio	Device Parameters							
14	Image	IP Camera Paramet	ters						
圁	Event	Import Config. File							
B	Storage	Device Parameters			Browse	Import			
8	VCA	Status				tion and			
		IP Camera Parameters Status			Browse	Import			
		Upgrade			Step 4: Clic	k 'Browse'			
		Firmware 🗸			Browse	Upgrade			

Step 1: Input the IP address to log into the web interface.

- Step 2: Click on the "Configuration" tab
- Step 3: Under the "System" menu, click on "Maintenance"
- Step 4: Under the "Upgrade" header, click on "Browse"



Title:	How to u vulnerab		le firmware to g	ard against potential	Version: 1	.0	Current	Date:	23/09/2021
Product:	Mixed pr	oduct	S					Page:	5 of 10
Action Required:	Informat	ion Or	nly						
	oc/page/config.as	sp			- d			<i>.</i> ۹	☆☆ ♥ 🙂
	1								
<b>*</b>									
	🙋 打开				×		<b>1</b> ad	min 🚯 Help	E+ Logout
	$\leftarrow \rightarrow \cdot \prime$	۲ » 📕 ۱	<sup>空</sup> 品类 > NVR > 76Q C >	ن v	٩				^
Local					• • 0				
System		,	* 名称	^ 修改日則					
System Settings									
Maintenance		- 1	digicap.dav	2021/6 STD_V4.31.102_210626.z 2021/9	/26 19:55 DA /23 16:39 Wit				
Security				e click the FW package.					
Camera Management			Step 5. Doubl	e ener the two puckage.					
User Management									
Network	•								
Video/Audio	•								
image		t (C:)							
Event		t (D:) t (E:)							
Storage Storage		-	~ <		>				
Co VCA									
		X	(件名(N): digicap.dav	× *.*	~				
				打开(O)	取消				
	Upgrade					Step 6: Cli	ck 'Upgrade'		
	Firmware V			Brot	vse Upgrade				Ť
							6	)英,🙂 🖉	· 📟 🐁 👕 🖌

Step 5: Choose the FW package on your PC. Please note that the FW package must be decompressed.

Step 6: Click on "Upgrade." The device will reboot automatically after upgrade is complete.



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	6 of 10
Action Required:	Information Only				

## Method 3: Upgrade Using Local GUI (NVRs)

NVR	۲		٥	⊁	踞 후 다 ()
		Device Name	Network Video Recorde		
		Firmware	V4.30.217, Build 210204	ŵ	
		Device Model	DS-7608NI-K1	×	
lite da a		Serial No.	0820210410CCRRF8243	31557WCVU	
	Simple	Restore		o default, except user	passwords and general network parameters.
stratio.	Factory	y Defaults	Restore all device param	neters to default settin	<u>g</u> s.
대학원공	Restore	to Inactive			eave all settings unchanged. Your admin password will
. 바람 바람 가슴					
				الترجيع المرجيع	이 바이 동물이 다니 동물이 했다.

Step 1: Go to Maintenance Tab.

Step 2: Click on the icon: 🏠

Step 3: Insert the USB drive with the FW package (this must be decompressed first); the NVR will then detect

the USB drive and show the files listed. Choose the FW package from the list.

Step 4: Click on "Upgrade." The device will reboot automatically after upgrade is complete.

Device Upgrade						×
.ocal Upgrade	Device Name	USB Flash Disk 1-1		File Format	*.dav;*.mav;*.iav	
Dnline Upgrade	🕁 Upgrade O Re	fresh				
	File Name			I Edit Date	I Delete	
			Folder	01-01-1970 00:0		
	🖪 digicap.dav	43.78MB		13-03-2021 17:1		



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	7 of 10
Action Required:	Information Only				

### Method 4: Online Upgrade Using Local GUI (NVRs)

Step 1: Enable the platform in Network > Hik-Connect



Step 2: After device is online, click on the "Update" button and enter the online upgrade interface

NVR	۲	ĨQ	¢	⋇	::: 다 나
		Device Name	Network Video Recorde	с	
		Firmware	V4.30.217, Build 210204	ŵ	
		Device Model	DS-7608NI-K1	*	
		Serial No.	0820210410CCRRF824	31557WCVU	
	Simple R	Restore	Restore all parameters (	o default, except user	passwords and general network parameters.
	Factory [	Defaults	Restore all device paran	neters to default setting	
	Restore to	Inactive	Restore the device to the	e inactive status, and l	eave all settings unchanged. Your admin password will



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	8 of 10
Action Required:	Information Only				

Device Upgrade		×
Local Upgrade	Auto Download	
Online Upgrade	Current Version V4.30.217, Build 210204 Test Upgrade	
	Latest Version NVR V4.31.102, Build 210626  Download  Ignore  Note Upgrade file downloaded.  Close	

Step 3: Click "Test Upgrade" to obtain latest version, then "Download" for the firmware file and your device will be upgraded.



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products		Page:	9 of 10	
Action Required:	Information Only				

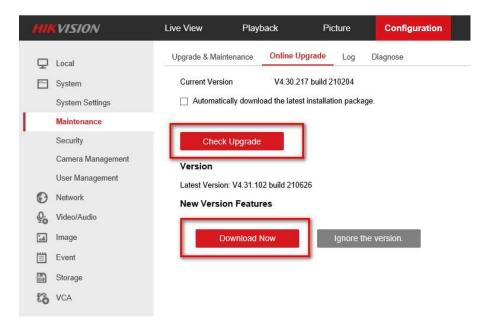
#### Method 5: Online Upgrade via Web Page

Step 1: First, use this path to enable the platform:

Configuration > Network > Advanced Settings > Platform Access

HI	VISION	Live View Play	/back Picture	Configuration
ç	Local	Email Platform Acce	ss Network Service 802.1	1x Other Integration Protocol Log Server Configuration
	System	Platform Access Mode	Hik-Connect	~
Ð	Network	Enable		
	Basic Settings	Server Address	litedev.sgp.hik-connect.co	m
	Advanced Settings	Register Status	Online	~
<u>Q.</u>	Video/Audio	Stream Encryption/Enc	ry	27944
<b>*</b>	Image		wed, including upper-case and nation of this alphabetical order	lower-case letters, and digits. To ensure device security, a combination are not allowed.
	Event	Enable Hik-Connec	t Server Time Sync	
	Storage			
6	VCA	🖹 Save		

Step 2: After the device is online, go to Configuration > Maintenance > Online Upgrade, click on "Check Upgrade" to obtain the latest version info; then download the firmware file to upgrade your device.



© 2021 Hikvision Canada Inc. All Rights Reserved. 2355 Skymark Ave, Suite 300, Mississauga, ON L4W 4Y6 • Phone: +1 866-200-6690 E-Mail: <u>techsupport.ca@hikvision.com</u> • www.hikvision.ca



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	10 of 10
Action Required:	Information Only				

**HIKVISION** 

Hikvision Canada Inc. <u>www.hikvision.ca</u> Technical Support Hotline: 1-855-655-9888