About Plural Security Vulnerabilities in SHARP Multifunctional Products (MFP)

Published: May 31, 2
Updated: October 15, 2

The following security vulnerabilities were identified and may impact some MFPs that are not properly protected with a strong admin passw and/or firewall. The following is a summary of the vulnerabilities, affected models, and countermeasures:

Vulnerability identification number	JVNVU#93051062 / See the following Detailed Information of the vulnerabilities for the CVE numbers
Affected models and firmware version	See the separate table below.
Detailed information of the vulnerabilities	CVE-2024-28038: Some device web pages may cause stack-based buffer overflow CVE-2024-28955: Permission is incorrectly assigned for the file in which some sensitive information is store and they can be viewed by exploiting another vulnerability CVE-2024-29146: Some sensitive information is stored as plain text and can be viewed by exploiting anothe vulnerability CVE-2024-29978: Some sensitive information is stored as plain text and can be viewed by exploiting anothe vulnerability CVE-2024-32151: Some sensitive information can be decrypted by exploiting another vulnerability CVE-2024-33605: Some device web pages may cause path traversal attacks CVE-2024-33610: Some device web pages have improper access control authority CVE-2024-33616: Improper credential information for executing some device feature may cause reference t internal information in the device CVE-2024-34162: Some device web pages may send credential information stored in the device unintentionally (This may be used by attackers who already hacked the device and obtained its authority.) CVE-2024-35244: Credential information for executing some device features are hard-coded and can be exploited by attackers who improperly obtained the credential information CVE-2024-36248: Credential information for accessing external sites are hard-coded and can be exploited b attackers who improperly obtained the credential information CVE-2024-36249: Some device web pages may cause cross-site scripting attacks CVE-2024-36251: Some device web pages may cause device hang-up due to out-of-bounds memory reference CVE-2024-36254: Some device web pages may cause device hang-up due to out-of-bounds memory reference CVE-2024-58388: Some device web pages may cause path traversal attacks (addressed by the same firmw update as CVE-2024-33605) (Updated: October 15, 2026)

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking

Do Not Sell or Share My Personal Information

Condition to enable attacks using this vulnerability	To enable attackers to successfully attack the MFP using these vulnerabilities, the following conditions shall b fulfilled: ● The attacker is able to access the corporate network to which the MFP is connected ● The attacker knows the information that users cannot know through normal operation
Possible impacts	If the above conditions are fulfilled, attackers may be able to : 1. execute arbitrary command codes on the MFP 2. read files and data in the programs on the MFP 3. access part of information on the MFP with unintended authority 4. execute cross-site scripting (XSS) on the MFP web page 5. hang the MFP up using crafted HTTP request on the MFP web page
Mitigation measures	To mitigate security risks and the command injection vulnerability, ensure to protect your MFPs and apply the following countermeasures: ● Change admin password from factory default and manage it appropriately. ● Do not connect MFPs directly to the Internet. Connect them via a firewall or similar network appliance. ● Restrict device web page access via password (enable [System Settings]-[Security Settings]-[Restrict Dev Web Page Access Via Password]). If the above countermeasures are not practiced, devices may be accessed by attackers and cause data leaka
Countermeasure	See [Affected models and the status of countermeasures] below. Sharp released updated firmware to mitigate these vulnerabilities for the models listed in Table 1. Regarding the models listed in Table 2, all firmware versi are affected, however, firmware support has ended. Please implement the above mitigation measures or consider discontinuing use of the product or migrating to a successor model. For details, consult your authoriz Sharp service providers.
Acknowledgment	We truly appreciate the following people who reported these vulnerabilities: Pierre Barre (CVE-2024-28038, CVE-2024-28955, CVE-2024-29146, CVE-2024-29978, CVE-2024-32151, CVE-2024-33605, CVE-2024-33610, CVE-2024-33616, CVE-2024-34162, CVE-2024-35244, CVE-2024-36248, CVE-2024-36251), Pontus Hassen security researcher at Omegapoint（https://omegapoint.se) (CVE-2024-33610), Morgan Davies of Cyber Security Specialists (https://www.cybersecurityspecialists.co.uk/) (CVE-2024-3624 Damien BOLUS – Torii Security (CVE-2024-36249), and Jarrod Stebick (CVE-2024-36254) (Updated: October 15, 2026)
Information	JVNVU#93051062: https://jvn.jp/en/vu/JVNVU93051062/index.html CVE: https://www.cve.org/CVERecord?id=CVE-2024-28038 https://www.cve.org/CVERecord?id=CVE-2024-28955 https://www.cve.org/CVERecord?id=CVE-2024-29146 https://www.cve.org/CVERecord?id=CVE-2024-29978 https://www.cve.org/CVERecord?id=CVE-2024-32151 https://www.cve.org/CVERecord?id=CVE-2024-33605 https://www.cve.org/CVERecord?id=CVE-2024-33610 https://www.cve.org/CVERecord?id=CVE-2024-33616 https://www.cve.org/CVERecord?id=CVE-2024-34162 https://www.cve.org/CVERecord?id=CVE-2024-35244 https://www.cve.org/CVERecord?id=CVE-2024-36248

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking

	https://www.cve.org/CVERecord?id=CVE-2024-36249 https://www.cve.org/CVERecord?id=CVE-2024-36251 https://www.cve.org/CVERecord?id=CVE-2024-36254 https://www.cve.org/CVERecord?id=CVE-2024-58388 (Updated: October 15, 2026)

(Updated: October 15, 2026)

● CVE-2024-58388 was published.
The issue was addressed by the same firmware update released for CVE-2024-33605.

● The reported CVE ID and the reporter details are corrected in Acknowledgment.

■ Affected models and the status of countermeasures

Table 1: Countermeasure firmware is available for the following models:

Category	Model name	Firmware version affected (see note) * Check the 2nd to 4th digits of the firmware version
Digital Full-color Multifunctional System	BP-90C70/BP-90C80 (Possible impact Nos. 1, 2 and 4 are not affected)	“200” or earlier
	BP-70C65/BP-70C55/BP-70C45/ BP-70C36/BP-70C31/ BP-60C45/BP-60C36/BP-60C31/ BP-50C65/BP-50C55/BP-50C45/ BP-50C36/BP-50C31/BP-50C26/ BP-55C26 (Possible impact No. 2 is not affected)	“310” or earlier
	MX-8081/MX-7081	“150” or earlier
	MX-6071/MX-5071/MX-4071/ MX-3571/MX-3071/ MX-4061/MX-3561/MX-3061/ MX-6051/MX-5051/MX-4051/ MX-3551/MX-3051/MX-2651/ MX-6071S/MX-5071S/MX-4071S/ MX-3571S/MX-3071S MX-4061S/MX-3561S/MX-3061S (Possible impact No. 2 is not affected)	“612” or earlier
	BP-30C25 BP-30C25Y BP-30C25Z BP-30C25T	“123” or earlier
	MX-7580N/MX-6580N	“502” or earlier
	MX-8090N/MX-7090N	“404” or earlier
	MX-6070N/MX-5070N/MX-4070N/ MX-3570N/MX-3070N/ MX-4060N/MX-3560N/MX-3060N/ MX-6070V/MX-5070V/MX-4070V/	“801” o

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking

	MX-3570V/MX-3070V/ MX-4060V/MX-3560V/MX-3060V/ MX-6070N A/MX-4070N A/MX-3070N A MX-6070V A/MX-4070V A/MX-3070V A	
	MX-6050N/MX-5050N/ MX-4050N/MX-3550N/MX-3050N/ MX-6050V/MX-5050V/ MX-4050V/MX-3550V/MX-3050V/ MX-2630N/ MX-3050N A/ MX-3050V A	“801” or earlier
	MX-C304W/MX-C303W/ MX-C304/MX-C303/ MX-C304WH/MX-C303WH	“512” or earlier
	DX-2500N/DX-2000U (Possible impacts Nos. 2, 4 and 5 are not affected)	“202” or earlier
Digital Multifunctional System (Monochrome)	BP-70M90/BP-70M75 (Possible impact No. 2 is not affected)	“303” or earlier
	BP-70M65/BP-70M55/BP-70M45/ BP-70M36/BP-70M31/ BP-50M65/BP-50M55/BP-50M45/ BP-50M36/BP-50M31/BP-50M26 (Possible impact No. 2 is not affected)	“310” or earlier
	MX-M1206/MX-M1056	“113” or earlier
	MX-M7570/MX-M6570	“455” or earlier
	MX-M6071/MX-M5071/MX-M4071/ MX-M3571/MX-M3071/ MX-M6051/MX-M5051/MX-M4051/ MX-M3551/MX-M3051/MX-M2651/ MX-M3571S/MX-M3071S/ MX-M6071S/MX-M5071S/MX-M4071S (Possible impact No. 2 is not affected)	“412” or earlier
	BP-30M35/BP-30M31/BP-30M28/ BP-30M35T/BP-30M31T/BP-30M28T	“211” or earlier
	MX-B476W/MX-B376W/ MX-B456W/MX-B356W/ MX-B476WH/MX-B376WH/ MX-B456WH/MX-B356WH	“412” or earlier
	MX-M905	“611” o
	MX-M6070/MX-M5070/MX-M4070/ MX-M3570/MX-M3070/ MX-M6050/MX-M5050/MX-M4050/	“502” o

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking

	MX-M3550/MX-M3050/ MX-M2630/ MX-M6070 A/MX-M4070 A/MX-M3070 A/ MX-M3050 A/ MX-M2630 A	
	BP-B550WD/BP-B540WR/ BP-B547WD/BP-B537WR (Possible impact No. 2 is not affected)	“250” or earlier
	MX-B455W/MX-B355W/ MX-B455WZ/MX-B355WZ/ MX-B455WT/MX-B355WT	“404” or earlier

NOTE: Follow the steps to check firmware version of your MFP.
Administrator login is required:

- Select [Settings] icon from the operation panel.
  If you are accessing the MFP from your PC within the network, you may access the MFP settings via Web browser by entering its IP address.
- Select [Status] tab.
  Select [Firmware version].
- The 16-digit alphanumeric string after “BUNDLE” (two 8-digit alphanumeric strings connected with an underscore) is the firmware version(e.g., 0510Z200_22040400).

Table 2: For the following models, firmware support has ended. Please implement the above mitigation measures or consider discontinuin use of the product or migrating to a successor model:

Category	Model name
Digital Full-color Multifunctional System	MX-7500N/MX-6500N (Possible impact Nos. 2 and 5 are not affected)
	MX-7040N/MX-6240N (Possible impact Nos. 2 and 5 are not affected)
	MX-5141N/MX-5140N/MX-4141N/MX-4140N/ MX-5141N A/MX-4140N A (Possible impact No. 2 is not affected)
	MX-3640N/MX-3140N/MX-2640N/MX-3140N A/ MX-3640NR/MX-3140NR/MX-2640NR (Possible impact Nos. 2 and 5 are not affected)
	MX-3116N/MX-2616N/ MX-3115N/MX-2615N/MX-2615 A (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-5112N/MX-5111N/MX-5110N/MX-4112N/MX-4111N/MX-41 (Possible impact Nos. 2 and 5 are not affected)
	MX-3610N/MX-3110N/MX-2610N/MX-3110N A/MX-3610NR (Possible impact Nos. 2 and 5 are not affected)

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking

	MX-C301W/MX-C301 (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-2314N/MX-2314NR (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-3111U/MX-2310U/MX-2310R (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-2010U/MX-1810U (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-C401/DX-C401/DX-C401 J/MX-C400/DX-C400/ MX-C381/DX-C381/MX-C380/MX-C381B MX-C312/MX-C311/DX-C311/DX-C311J/MX-C310/DX-C310/ MX-C400P/MX-C380P/ MX-C402SC/MX-C382SC/MX-C382SCB (Possible impacts Nos. 2, 4 and 5 are not affected)
	MX-5001N/MX-5000N/MX-4101N/MX-4100N (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-3100N/MX-3100G/MX-2600N/MX-2600G (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-3101N/MX-2601N/MX-2301N (Possible impact Nos. 2, 4 and 5 are not affected)
Digital Multifunctional System (Monochrome)	MX-M1205/MX-M1055 (Possible impact Nos. 2 and 5 are not affected)
	MX-M1204/MX-M1054/MX-M904 (Possible impact Nos. 2 and 5 are not affected)
	MX-M754N/MX-M654N/MX-M754N A/MX-M654N A (Possible impact No. 2 is not affected)
	MX-M565N/MX-M465N/MX-M365N/ MX-M465N A/MX-M365N A (Possible impact No. 2 is not affected)
	MX-M564N/MX-M464N/MX-M364N/MX-M564N A (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-M356N/MX-M316N/MX-M315N/MX-M356U/MX-M315U/ MX-M266N/MX-M265N/MX-M265U/ MX-M315NE/MX-M265NE/ MX-M356NV/MX-M316NV/MX-M315NV/MX-M356UV/MX-M315UV/ MX-M266NV/MX-M265NV/MX-M265UV/ MX-M315NE/MX-M265NE/MX-M315V/MX-M265V (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-M354N/MX-M314N/MX-M264N/ MX-M354U/MX-M314U/MX-M264U/ MX-M314NV/MX-M264NV/

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking

	MX-M354NR/MX-M314NR/MX-M264NR (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-B402/MX-B382/ MX-B402P/MX-B382P/ MX-B402SC/MX-B382SC (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-B401/MX-B381/ MX-B400P/MX-B380P (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-M753N/MX-M753U/MX-M623N/MX-M623U (Possible impact Nos. 2, 4 and 5 are not affected)
	MX-M503N/MX-M453N/MX-M363N/MX-M283N/ MX-M503U/MX-M453U/MX-M363U (Possible impact Nos. 2, 4 and 5 are not affected)

© SHARP CORPORATION

We use your personal information such as unique personal identifier and information regarding your use of our website through cookies and other tracking