CVE-2026-1789

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-1789
State	PUBLISHED
Assigner	Canon
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 00:16:26 UTC
Updated	2026-04-24 14:39:56 UTC
Description	A vulnerability in the browser-based remote management interface may allow an administrator to access sensitive informati

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from f98c90f0-e9bd-4fa7-911b-51993f3571fd

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-807 | CWE-807 CWE-807: Reliance on Untrusted Inputs in a Security Decision

Version	Source	Type	Score	Severity	Vector
4.0	f98c90f0-e9bd-4fa7-911b-51993f3571fd	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N
3.1	f98c90f0-e9bd-4fa7-911b-51993f3571fd	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Canon Inc.	ImagePRESS Series	affected all version	Not specified
CNA	Canon Inc.	ImageFORCE Series	affected all version	Not specified
CNA	Canon Inc.	ImageRUNNER ADVANCE Series	affected all version	Not specified
CNA	Canon Inc.	ImageRUNNER Series	affected all version	Not specified
CNA	Canon Inc.	Satera MF735Cx	affected v15.00 or earlier	Not specified

CNA	Canon Inc.	Satera MF7525F	affected v15.00 or earlier	Not specified
CNA	Canon Inc.	Satera MF7625F	affected v8.12 or earlier	Not specified
CNA	Canon Inc.	Satera MF7725F	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	Satera MF842CDW	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	ImageCLASS X C1538iF II	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	ImageCLASS X MF1538C II	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	I-SENSYS C1533iF II	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	I-SENSYS X C1538 IF II	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	I-SENSYS MF842Cdw	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	MF842CDW	affected v16.04 or earlier	Not specified
CNA	Canon Inc.	MF842CX	affected v16.04 or earlier	Not specified

References

Reference	Source	Link
psirt.canon/advisory-information/cp2026-003	f98c90f0-e9bd-4fa7-911b-51993f3571fd	psirt.canon
www.canon-europe.com/support/product-security	f98c90f0-e9bd-4fa7-911b-51993f3571fd	www.canon
canon.jp/support/support-info/260423vulnerability-response	f98c90f0-e9bd-4fa7-911b-51993f3571fd	canon.jp
www.usa.canon.com/about-us/to-our-customers/cpa2026-003-vulnerability-mitigatio...	f98c90f0-e9bd-4fa7-911b-51993f3571fd	www.usa.c
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.