



Sangfor Operation and Maintenance Security Management System HTTP POST Request get_clip_img command injection

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2026-1412
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-26 01:15:49 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability has been found in Sangfor Operation and Maintenance Security Management System up to 3.0.12. The impo

Risk And Classification					
Primary CVSS: v4.0 5.5 MEDIUM from cna@vuldb.com					
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X					
Problem Types: CWE-74 CWE-77 CWE-77 Command Injection CWE-74 Injection					
Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	5.5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown	
Attack Vector	Network
Attack Complexity	

Low
Attack Requirements
None
Privileges Required
None
User Interaction
None
Confidentiality
Low
Integrity
Low
Availability
Low
Sub Conf.
None
Sub Integrity
None
Sub Availability
None
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/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
None
User Interaction
None
Scope
Unchanged
Confidentiality
High
Integrity
High
Availability
High
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

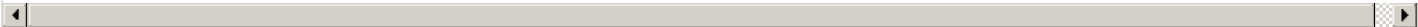
Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sangfor	Operation And Maintenance Security Management System	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.0	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.1	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.2	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.3	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.4	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.5	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.6	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.7	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.8	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.9	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.10	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.11	Not specified
CNA	Sangfor	Operation And Maintenance Security Management System	affected 3.0.12	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Required, VDB Entry
github.com/LX-LX88/cve/issues/22	cna@vuldb.com	github.com	Exploit, Issue Tracking, Third Party Advisory
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: hhs34 (VulDB User) (en)

Additional Advisory Data		
Source	Time	Event
CNA	2026-01-25T00:00:00.000Z	Advisory disclosed
CNA	2026-01-25T01:00:00.000Z	VulDB entry created
CNA	2026-01-31T07:44:08.000Z	VulDB entry last update

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