Tiandy Easy7 Integrated Management Platform Configuration ImportSystemConfiguration.jsp os command injection

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

Summary

CVE	CVE-2026-4585
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 12:16:25 UTC
Updated	2026-04-24 16:32:53 UTC
Description	A vulnerability has been found in Tiandy Easy7 Integrated Management Platform up to 7.17.0. This vulnerability affects unk

Risk And Classification

Primary CVSS: v4.0 8.9 HIGH from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.002100000 probability, percentile 0.433660000 (date 2026-04-26)

Problem Types: CWE-77 | CWE-78 | CWE-78 OS Command Injection | CWE-77 Command Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	8.9	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/C
4.0	CNA	DECLARED	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	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	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R
3.0	CNA	DECLARED	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	DECLARED	10		AV:N/AC:L/Au:N/C:C/I:C/A:C/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

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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/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

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.0	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.1	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.2	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.3	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.4	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.5	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.6	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.7	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.8	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.9	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.10	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.11	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.12	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.13	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.14	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.15	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.16	Not specified
CNA	Tiandy	Easy7 Integrated Management Platform	affected 7.17.0	Not specified

CNA	Handy	Easy7 Integrated Management Platform	affected 7.1.7.0	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	
vuldb.com	cna@vuldb.com	vuldb.com	
my.feishu.cn/docx/WkHjd3oajoIw5exHk9ecUHaFnKd	cna@vuldb.com	my.feishu.cn	
vuldb.com	cna@vuldb.com	vuldb.com	
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: red88-debug (VulDB User) (en)

CNA: VulDB (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-22T00:00:00.000Z	Advisory disclosed
CNA	2026-03-22T01:00:00.000Z	VulDB entry created
CNA	2026-03-22T10:32:54.000Z	VulDB entry last update

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**