Openfind | MailGates/MailAudit - Stack-based Buffer Overflow

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

Summary

CVE	CVE-2026-6350
State	PUBLISHED
Assigner	twcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 03:16:30 UTC
Updated	2026-04-17 15:38:09 UTC
Description	MailGates/MailAudit developed by Openfind has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated rem

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from twcert@cert.org.tw

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: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

EPSS: 0.000580000 probability, percentile 0.182410000 (date 2026-04-21)

Problem Types: CWE-121 | CWE-121 CWE-121 Stack-based buffer overflow

Version	Source	Type	Score	Severity	Vector
4.0	twcert@cert.org.tw	Secondary	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:X/
4.0	CNA	CVSS	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
3.1	twcert@cert.org.tw	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	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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: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

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Openfind	MailGates	affected 6.0 6.1.10.054 custom	Not specified
CNA	Openfind	MailGates	affected 5.0 5.2.10.099 custom	Not specified
CNA	Openfind	MailAudit	affected 6.0 6.1.10.054 custom	Not specified

CNA	Openfind	MailAudit	affected 5.0 5.2.10.099 custom	Not specified

References

Reference	Source	Link	Tags
www.twcert.org.tw/tw/cp-132-10844-1405d-1.html	twcert@cert.org.tw	www.twcert.org.tw	
www.twcert.org.tw/en/cp-139-10843-9ff91-2.html	twcert@cert.org.tw	www.twcert.org.tw	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: MailGates/MailAudit 6.0： Update to version 6.1.10.054 or later MailGates/MailAudit 5.0： Update to version 5.2.10.099 or later

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