OPEXUS eComplaint unauthenticated file upload

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-32867
State	PUBLISHED
Assigner	cisa-cg
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-19 16:16:03 UTC
Updated	2026-03-30 13:10:38 UTC
Description	OPEXUS eComplaint before version 10.1.0.0 allows an unauthenticated attacker to obtain or guess an existing case numbe

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from 9119a7d8-5eab-497f-8521-727c672e3725

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/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: 0.000550000 probability, percentile 0.171240000 (date 2026-04-01)

Problem Types: CWE-425 | CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key | CWE-425 CWE-425 Direct Request ('Forced Browsing')

Version	Source	Type	Score	Severity	Vector
4.0	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/
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	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

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:P/VC:N/VI:L/VA:L/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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opexustech	Ecase Ecomplaint	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OPEXUS	EComplaint	affected 10.1.0.0 custom	Not specified
CNA	OPEXUS	EComplaint	unaffected 10.1.0.0	Not specified

References

Reference	Source
raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-26-077-01.json	9119a7d8-5eab-497f-8521-727c672e3725
www.cve.org/CVERecord	9119a7d8-5eab-497f-8521-727c672e3725
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Adam Rose, CISA (en)

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