OPEXUS eComplaint and eCase insecure password reset

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-32865
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 13:12:06 UTC
Description	OPEXUS eComplaint and eCASE before version 10.1.0.0 include the secret verification code in the HTTP response when r

Risk And Classification

Primary CVSS: v4.0 9.2 CRITICAL from 9119a7d8-5eab-497f-8521-727c672e3725

CVSS:4.0/AV:N/AC:L/AT:P/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: 0.000540000 probability, percentile 0.170840000 (date 2026-04-01)

Problem Types: CWE-200 | CWE-640 | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor | CWE-640 CWE-640 Weak Password Recovery Mechanism for Forgotten Password

Version	Source	Type	Score	Severity	Vector
4.0	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/
4.0	CNA	DECLARED	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/
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	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

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Attack Requirements

Present

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:P/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

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
CNA	OPEXUS	ECASE	affected 10.1.0.0 custom	Not specified
CNA	OPEXUS	ECASE	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.