PredatorSense V3: Local Privilege Escalation (LPE) vulnerability

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

Summary

CVE	CVE-2026-8069
State	PUBLISHED
Assigner	Acer
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 07:16:29 UTC
Updated	2026-05-08 07:16:29 UTC
Description	PredatorSense version 3.00.3136 to 3.00.3196 contain Local Privilege Escalation (LPE) vulnerability.The program exposes

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from 8fc372e3-d9c5-46e4-9410-38469745c639

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/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

Problem Types: CWE-22 | CWE-269 | CWE-284 | CWE-732 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-269 CWE-269: Improper Privilege Management | CWE-284 CWE-284: Improper Access Control | CWE-732 CWE-732: Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
4.0	8fc372e3-d9c5-46e4-9410-38469745c639	Secondary	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H
4.0	CNA	CVSS	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Acer	PredatorSense V3	affected 3.00.3136 3.00.3196 custom	Windows

References

Reference	Source	Link	Tags
community.acer.com/en/kb/articles/19652	8fc372e3-d9c5-46e4-9410-38469745c639	community.acer.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: Artem Domarev (en)

Additional Advisory Data

Solutions

CNA: Update to version 3.00.3198.

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

Free CVE JSON API cve.report/api

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