



CVE-2015-4027

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-4027
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-17 19:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The AcuWVSSchedulerv10 service in Acunetix Web Vulnerability Scanner (WVS) before 10 build 20151125 allows local us

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acunetix	Web Vulnerability Scanner	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
Acunetix WVS 10 - Local Privilege Escalation - Windows local Exploit				af854a3a-2127-4...
Acunetix build includes security checks in CORS configurations, Rails web applications and identifies the vBulletin 5 RCE				af854a3a-2127-4...
Acunetix WVS 10 Local Privilege Escalation ≈ Packet Storm				af854a3a-2127-4...
CVE Program record				CVE.ORG
NVD vulnerability detail				NVD
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				