CVE-2014-3272

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

Summary

CVE	CVE-2014-3272
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-26 00:25:31 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Agent in Cisco Tidal Enterprise Scheduler (TES) 6.1 and earlier allows local users to gain privileges via crafted Tidal Jo

Risk And Classification

Primary CVSS: v2.0 6 from nvd@nist.gov

AV:L/AC:H/Au:S/C:C/I:C/A:C

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:H/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Tidal Enterprise Scheduler	3.0.0	All	All	All

Application	Cisco	Tidal Enterprise Scheduler	3.0.1	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	5.2.2	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	5.3.0	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	5.3.1	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	6.0.0	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	6.0.1	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	6.0.2	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	6.0.3	All	All	All
Application	Cisco	Tidal Enterprise Scheduler	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
Cisco Tidal Enterprise Scheduler Agent Input Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-4
Security Advisory SA58922 - Cisco Tidal Enterprise Scheduler Agent TJB Privilege Escalation Vulnerability - Secunia	af854a3a-2127-4
Cisco Security Notice: Cisco Tidal Enterprise Scheduler Agent Privilege Escalation Vulnerability	af854a3a-2127-4
Alert Details - Security Center - Cisco Systems	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.