CVE-2019-12532

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

Summary

CVE	CVE-2019-12532
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-26 18:15:00 UTC
Updated	2022-04-29 12:30:00 UTC
Description	Improper access control in the Insyde software tools may allow an authenticated user to potentially enable escalation of priv

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Insyde	H2oelv	All	All	All	All
Application	Insyde	H2oelv	All	All	All	All
Application	Insyde	H2offt	All	All	All	All
Application	Insyde	H2offt	All	All	All	All
Application	Insyde	H2offt	All	All	All	All
Application	Insyde	H2ooae	All	All	All	All
Application	Insyde	H2ooae	All	All	All	All
Application	Insyde	H2opcm	All	All	All	All
Application	Insyde	H2opcm	All	All	All	All
Application	Insyde	H2osde	All	All	All	All
Application	Insyde	H2osde	All	All	All	All
Application	Insyde	H2ouve	All	All	All	All
Application	Insyde	H2ouve	All	All	All	All

References

Reference	Source	Link	Tags
Screwed Drivers – Signed, Sealed, Delivered - Eclypsium	MISC	eclypsium.com	Third Party Ac

CVE-2019-12532 InsydeH2O Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
Security Advisory | Insyde Software	CONFIRM	www.insyde.com	Vendor Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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