CVE-2019-3941

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

Summary

CVE	CVE-2019-3941
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-09 16:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Advantech WebAccess 8.3.4 allows unauthenticated, remote attackers to delete arbitrary files via IOCTL 10005 RPC.

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	Webaccess	8.3.4	All	All	All
Application	Advantech	Webaccess	8.3.4	All	All	All

References

Reference	Source	Link	Tags
Multiple Advantech WebAccess Vulnerabilities - Research Advisory | Tenable®	MISC	www.tenable.com	Exploit, Third Party A
Advantech WebAccess Multiple Security Vulnerabilities	BID	www.securityfocus.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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