CVE-2006-3896

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

Summary

CVE	CVE-2006-3896
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-19 19:28:00 UTC
Updated	2011-03-08 02:39:00 UTC
Description	The NeoScale Systems CryptoStor 700 series appliance before 2.6 relies on client-side ActiveX code for smartcard authent

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Neoscale Systems	Cryptostor Tape 700	All	All	All	All
Hardware	Neoscale Systems	Cryptostor Tape 700	All	All	All	All

References

Reference	Sourc
NeoScale Systems CryptoStor Tape 700 Series Appliance SmartCard Authentication Bypass Vulnerability	BID
US-CERT Vulnerability Note VU#339004	CERT
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
NeoScale Systems CryptoStor 700 Series Security Bypass Weakness - Advisories - Secunia	SECU
SecurityTracker.com Archives - NeoScale CryptoStor 700 Series Appliance Lets Remote Users Bypass Token-Based Authentication	SECT
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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