



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 authentication.

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	Source
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)