CVE-2001-0856

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2001-0856
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-12-06 05:00:00 UTC
Updated	2016-10-18 02:12:00 UTC
Description	Common Cryptographic Architecture (CCA) in IBM 4758 allows an attacker with physical access to the system and Combin

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ibm	4758	All	All	All	All
Hardware	Ibm	4758	All	All	All	All

References

Reference	Source	Link	Tags
Extracting a 3DES key from an IBM 4758	MISC	www.cl.cam.ac.uk	Patch, Vendor Advisory
IBM CCA 3DES Exporter Key Generation Weakness	BID	www.securityfocus.com	
Extracting a 3DES key from an IBM 4758	MISC	www.cl.cam.ac.uk	Exploit, Vendor Advisory
20011109 Extracting a 3DES key from an IBM 4758	BUGTRAQ	marc.info	
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.

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