CVE-2018-6622

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-6622
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-17 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered that affects all producers of BIOS firmware who make a certain realistic interpretation of an obscu

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trustedcomputinggroup	Trusted Platform Module	2.0	All	All	All
Application	Trustedcomputinggroup	Trusted Platform Module	2.0	All	All	All

References

Reference	Source	Link	Tags
Trusted Platform Module (TPM) CVE-2018-6622 Local Security Vulnerability	BID	www.securityfocus.com	Third Party Ac
A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping | USENIX	MISC	www.usenix.org	Third Party Ac
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.

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