CVE-2018-5382

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-5382
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-16 14:29:00 UTC
Updated	2022-04-20 15:31:00 UTC
Description	The default BKS keystore use an HMAC that is only 16 bits long, which can allow an attacker to compromise the integrity of

Risk And Classification

Problem Types: CWE-354

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-crytography-api	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-crytography-api	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-crytography-api	All	All	All	All
Application	Redhat	Satellite	6.4	All	All	All
Application	Redhat	Satellite Capsule	6.4	All	All	All

References

Reference	Source	Link	Tags
VU#306792 - Bouncy Castle BKS-V1 keystore files vulnerable to trivial hash collisions	CERT-VN	www.kb.cert.org	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
bouncycastle.org	MISC	www.bouncycastle.org	Vendor Advis
Bouncy Castle BKS-V1 CVE-2018-5382 Security Weakness	BID	www.securityfocus.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

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