CVE-2017-5972

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

Summary

CVE	CVE-2017-5972
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-14 06:59:00 UTC
Updated	2020-07-31 20:35:00 UTC
Description	The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fa

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
SYN Flood Mitigation with synsanity | GitHub Engineering	MISC	githuber
Linux Kernel 3.10.0 (CentOS7) - Denial of Service	EXPLOIT-DB	www.exp
CVE-2017-5972	MISC	security-
CentOS7 Kernel Denial Of Service ≈ Packet Storm	MISC	packetst
CentOS7 kernel crashing by rsyslog daemon vulnerability DoS - CXSecurity.com	MISC	cxsecuri
1422081 – (CVE-2017-5972) CVE-2017-5972 kernel: SYN cookie protection mechanism not properly implemented	MISC	bugzilla.
oss-sec: Concerns about CVE-2017-5972	MISC	seclists.
CVE-2017-5972 - Red Hat Customer Portal	MISC	access.r
Linux Kernel CVE-2017-5972 Denial of Service Vulnerability	BID	www.sec
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

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**