CVE-2016-5418

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-5418
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-21 14:25:00 UTC
Updated	2019-12-27 16:08:00 UTC
Description	The sandboxing code in libarchive 3.2.0 and earlier mishandles hardlink archive entries of non-zero data size, which might a

Risk And Classification

Problem Types: CWE-20 | CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libarchive	Libarchive	All	All	All	All
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Openshift	3.1	All	All	All
Application	Redhat	Openshift	3.2	All	All	All
Application	Redhat	Openshift	3.1	All	All	All
Application	Redhat	Openshift	3.2	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	acce
Red Hat Customer Portal	REDHAT	rhn.
Hard links with data can evade sandboxing restrictions · Issue #746 · libarchive/libarchive · GitHub	CONFIRM	githu
Oracle Linux Bulletin - July 2016	CONFIRM	www
Red Hat Customer Portal	REDHAT	acce
Red Hat Customer Portal	REDHAT	rhn.
Fixes for Issue #745 and Issue #746 from Doran Moppert. · libarchive/libarchive@dfd6b54 · GitHub	CONFIRM	githu
Bug 1362601 – CVE-2016-5418 libarchive: Archive Entry with type 1 (hardlink), but has a non-zero data size file overwrite	CONFIRM	bug
libarchive: Multiple vulnerabilities (GLSA 201701-03) — Gentoo security	GENTOO	secu
oss-security - FreeBSD update components vulns (libarchive, bsdiff, portsnap)	MLIST	www
FreeBSD · GitHub	MISC	gist.
libarchive CVE-2016-5418 Arbitrary File Write Vulnerability	BID	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710502 Gentoo Linux libarchive Multiple Vulnerabilities (GLSA 201701-03)