CVE-2017-12163

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

Summary

CVE	CVE-2017-12163
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 16:29:00 UTC
Updated	2023-02-12 23:27:00 UTC
Description	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.1

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	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 Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	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
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Gluster Storage	3.0	All	All	All
Application	Redhat	Gluster Storage	3.0	All	All	All
Application	Samba	Samba	All	All	All	All
Application	Samba	Samba	All	All	All	All

References

Reference
Red Hat Customer Portal
Document Display | HPE Support Center
1491206 – (CVE-2017-12163) CVE-2017-12163 Samba: Server memory information leak over SMB1
Samba - Security Announcement Archive
Samba CVE-2017-12163 Arbitrary File Write Vulnerability
Synology-SA-17:57 Samba | Synology Inc.
Document Display | HPE Support Center
Red Hat Customer Portal
Debian -- Security Information -- DSA-3983-1 samba
CVE-2017-12163 - Red Hat Customer Portal
Red Hat Customer Portal
Bug 1491206 – CVE-2017-12163 Samba: Server memory information leak over SMB1
Red Hat Customer Portal
Samba Multiple Flaws Let Remote Users Hijack Connections and Remote Authenticated Users Obtain Potentially Sensitive Information - Secu
September 2017 Samba Vulnerabilities in NetApp StorageGRID Products | NetApp Product Security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378135 Virtuozzo Linux Security Update for samba4-common (VZLSA-2017:2791)
- 378151 Virtuozzo Linux Security Update for samba-winbind-krb5-locator (VZLSA-2017:2789)
- 500632 Alpine Linux Security Update for samba
- 504396 Alpine Linux Security Update for samba