CVE-2015-7547

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-7547
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-18 21:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Libr

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.0.0	All	All	All
Application	F5	Big-ip Analytics	12.0.0	All	All	All
Application	F5	Big-ip Analytics	12.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	12.0.0	All	All	All

Application	F5	Big-ip Application Security Manager	12.0.0	All	All	All
Application	F5	Big-ip Domain Name System	12.0.0	All	All	All
Application	F5	Big-ip Domain Name System	12.0.0	All	All	All
Application	F5	Big-ip Link Controller	12.0.0	All	All	All
Application	F5	Big-ip Link Controller	12.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.0.0	All	All	All
Application	Gnu	Glibc	2.10	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All
Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12	All	All	All
Application	Gnu	Glibc	2.12.1	All	All	All
Application	Gnu	Glibc	2.12.2	All	All	All
Application	Gnu	Glibc	2.13	All	All	All
Application	Gnu	Glibc	2.14	All	All	All
Application	Gnu	Glibc	2.14.1	All	All	All
Application	Gnu	Glibc	2.15	All	All	All
Application	Gnu	Glibc	2.16	All	All	All
Application	Gnu	Glibc	2.17	All	All	All
Application	Gnu	Glibc	2.18	All	All	All
Application	Gnu	Glibc	2.19	All	All	All
Application	Gnu	Glibc	2.20	All	All	All
Application	Gnu	Glibc	2.21	All	All	All
Application	Gnu	Glibc	2.22	All	All	All
Application	Gnu	Glibc	2.9	All	All	All
Application	Gnu	Glibc	2.10	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All

Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12	All	All	All
Application	Gnu	Glibc	2.12.1	All	All	All
Application	Gnu	Glibc	2.12.2	All	All	All
Application	Gnu	Glibc	2.13	All	All	All
Application	Gnu	Glibc	2.14	All	All	All
Application	Gnu	Glibc	2.14.1	All	All	All
Application	Gnu	Glibc	2.15	All	All	All
Application	Gnu	Glibc	2.16	All	All	All
Application	Gnu	Glibc	2.17	All	All	All
Application	Gnu	Glibc	2.18	All	All	All
Application	Gnu	Glibc	2.19	All	All	All
Application	Gnu	Glibc	2.20	All	All	All
Application	Gnu	Glibc	2.21	All	All	All
Application	Gnu	Glibc	2.22	All	All	All
Application	Gnu	Glibc	2.9	All	All	All
Application	Hp	Helion Openstack	1.1.1	All	All	All
Application	Hp	Helion Openstack	2.0.0	All	All	All
Application	Hp	Helion Openstack	2.1.0	All	All	All
Application	Hp	Helion Openstack	1.1.1	All	All	All
Application	Hp	Helion Openstack	2.0.0	All	All	All
Application	Hp	Helion Openstack	2.1.0	All	All	All
Application	Hp	Server Migration Pack	7.5	All	All	All
Application	Hp	Server Migration Pack	7.5	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Oracle	Exalogic Infrastructure	1.0	All	All	All
Application	Oracle	Exalogic Infrastructure	2.0	All	All	All
Application	Oracle	Exalogic Infrastructure	1.0	All	All	All
Application	Oracle	Exalogic Infrastructure	2.0	All	All	All
Operating System	Oracle	Fujitsu M10 Firmware	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	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	7.0	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	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Sophos	Unified Threat Management Software	9.319	All	All	All
Application	Sophos	Unified Threat Management Software	9.355	All	All	All
Application	Sophos	Unified Threat Management Software	9.319	All	All	All
Application	Sophos	Unified Threat Management Software	9.355	All	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp4	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All

Operating System	Suse	Linux Enterprise Server	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All

References

Reference
Oracle Critical Patch Update Advisory - April 2016
Document Display | HPE Support Center
Vulnerability Note VU#457759 - glibc vulnerable to stack buffer overflow in DNS resolver
'[security bulletin] HPSBGN03549 rev.1 - HP IceWall Products using glibc, Remote Denial of Service (D' - MARC
[security-announce] openSUSE-SU-2016:0512-1: critical: Security update f
[security-announce] SUSE-SU-2016:0470-1: important: Security update for
CVE-2015-7547 - Red Hat Customer Portal
Bug 1293532 – CVE-2015-7547 glibc: getaddrinfo stack-based buffer overflow
Red Hat Customer Portal
UTM Up2Date 9.355 released | Sophos Blog
Red Hat Customer Portal
GNU glibc 'getaddrinfo()' Function Multiple Stack Buffer Overflow Vulnerabilities
Citrix Security Advisory for glibc Vulnerability CVE-2015-7547
[SECURITY] Fedora 22 Update: glibc-2.21-11.fc22
glibc getaddrinfo Stack-Based Buffer Overflow ≈ Packet Storm
Document Display | HPE Support Center
UTM Up2Date 9.319 released | Sophos Blog
Document Display | HPE Support Center
Red Hat Customer Portal
[R1] Portable SDK for UPnP Devices (libupnp) glibc Implementation getaddrinfo() Function Remote Stack Overflow - Research Advisory | Ten
McAfee KnowledgeBase - Intel Security - Security Bulletin: glibc vulnerabilities CVE-2015-5229 and CVE-2015-7547

McAfee KnowledgeBase - Intel Security - Security Bulletin: glibc vulnerabilities CVE-2015-5229 and CVE-2015-7547

[SECURITY] Fedora 23 Update: glibc-2.22-9.fc23

Moxa Command Injection / Cross Site Scripting / Vulnerable Software ≈ Packet Storm

Siemens Industrial Products glibc Library Vulnerability (Update C) | ICS-CERT

Oracle Critical Patch Update - January 2018

Page Not Found - Lenovo Support US

Full Disclosure: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X

Red Hat Customer Portal

Document Display | HPE Support Center

Document Display | HPE Support Center

Red Hat Customer Portal

Cisco Device Hardcoded Credentials / GNU glibc / BusyBox ≈ Packet Storm

USN-2900-1: GNU C Library vulnerability | Ubuntu

[security-announce] SUSE-SU-2016:0472-1: important: Security update for

Document Display | HPE Support Center

Document Display | HPE Support Center

18665 – (CVE-2015-7547) In send_dg, the recvfrom function is NOT always using the buffer size of a newly created buffer (CVE-2015-7547)

Carlos O'Donell - [PATCH] CVE-2015-7547 --- glibc getaddrinfo() stack-based buffer overflo

Bugtraq: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X

Security Advisory - GNU Glibc Buffer Overflow Security Vulnerability

[security-announce] openSUSE-SU-2016:0511-1: critical: Security update f

Glibc getaddrinfo() Stack Overflow Lets Remote or Local Users Execute Arbitrary Code - SecurityTracker

Debian -- Security Information -- DSA-3481-1 glibc

'[security bulletin] HPSBGN03547 rev.1 - HPE Helion Eucalyptus Node Controller and other Helion Eucal' - MARC

GNU C Library: Multiple vulnerabilities (GLSA 201602-02) — Gentoo Security

Red Hat Customer Portal

Broadcom Support Portal

Google Online Security Blog: CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow

[security-announce] SUSE-SU-2016:0473-1: important: Security update for

Nexans FTTO GigaSwitch Outdated Components / Hardcoded Backdoor ≈ Packet Storm

Document Display | HPE Support Center

SOL47098834 - glibc vulnerability CVE-2015-7547

Document Display | HPE Support Center

Public KB - SA40161 - [Pulse Secure] glibc getaddrinfo stack-based buffer overflow (CVE-2015-7547)

[security-announce] openSUSE-SU-2016:0510-1: important: Security update

'[security bulletin] HPSBGN03442 rev.1 - HP Helion OpenStack using glibc, Remote Denial of Service (D' - MARC

StruxureWare Data Center Operation Software Vulnerability Fixes - User Assistance for StruxureWare Data Center Operation 8 - Help Center
FortiGuard
CVE-2015-7547 GNU C Library (glibc) Vulnerability in Multiple NetApp Products | NetApp Product Security
'[security bulletin] HPSBGN03582 rev.1 - HPE Helion CloudSystem using glibc, Remote Code Execution, D' - MARC
Critical security flaw: glibc stack-based buffer overflow in getaddrinfo() (CVE-2015-7547) - Red Hat Customer Portal
Arista - Security Advisory 0017
Oracle Linux Bulletin - January 2016
Full Disclosure: SEC Consult SA-20210901-0 :: Multiple vulnerabilities in MOXA devices
Document Display | HPE Support Center
glibc - 'getaddrinfo' Remote Stack Buffer Overflow
Document Display | HPE Support Center
FortiGuard
'[security bulletin] HPSBGN03551 rev.1 - HPE Helion Development Platform using glibc, Remote Denial o' - MARC
VMSA-2016-0002 | United States
Document Display | HPE Support Center
Document Display | HPE Support Center
glibc - getaddrinfo Stack-Based Buffer Overflow
[security-announce] SUSE-SU-2016:0471-1: important: Security update for
Red Hat Customer Portal
Document Display | HPE Support Center
Document Display | HPE Support Center
Debian -- Security Information -- DSA-3480-1 eglibc
Red Hat Customer Portal
Full Disclosure: SEC Consult SA-20220615-0 :: Hardcoded Backdoor User and Outdated Software Components in Nexans FTTO GigaSwitch
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

43886 Huawei Router and Switch Buffer Overflow Vulnerability (Huawei-SA-20160304-01-glibc-en)

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