



CVE-2015-0235

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2015-0235
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-28 19:59:00 UTC
Updated	2022-07-05 18:42:00 UTC
Description	Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, all

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Ibm	Pureapplication System	1.0.0.0	All	All	All
Application	Ibm	Pureapplication System	1.1.0.0	All	All	All
Application	Ibm	Pureapplication System	2.0.0.0	All	All	All
Application	Ibm	Pureapplication System	1.0.0.0	All	All	All
Application	Ibm	Pureapplication System	1.1.0.0	All	All	All
Application	Ibm	Pureapplication System	2.0.0.0	All	All	All
Application	Ibm	Security Access Manager For Enterprise Single Sign-on	8.2	All	All	All
Application	Ibm	Security Access Manager For Enterprise Single Sign-on	8.2	All	All	All
Application	Oracle	Communications Application Session Controller	All	All	All	All

Application	Oracle	Communications Application Session Controller	3.7.1	-	All	All
Application	Oracle	Communications Application Session Controller	All	All	All	All
Application	Oracle	Communications Application Session Controller	3.7.1	-	All	All
Application	Oracle	Communications Eagle Application Processor	16.0	All	All	All
Application	Oracle	Communications Eagle Application Processor	16.0	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.0	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.0	All	All	All
Application	Oracle	Communications Lsms	13.1	All	All	All
Application	Oracle	Communications Lsms	13.1	All	All	All
Application	Oracle	Communications Policy Management	10.4.1	All	All	All
Application	Oracle	Communications Policy Management	11.5	All	All	All
Application	Oracle	Communications Policy Management	12.1.1	All	All	All
Application	Oracle	Communications Policy Management	9.7.3	All	All	All
Application	Oracle	Communications Policy Management	9.9.1	All	All	All
Application	Oracle	Communications Policy Management	10.4.1	All	All	All
Application	Oracle	Communications Policy Management	11.5	All	All	All
Application	Oracle	Communications Policy Management	12.1.1	All	All	All
Application	Oracle	Communications Policy Management	9.7.3	All	All	All
Application	Oracle	Communications Policy Management	9.9.1	All	All	All
Application	Oracle	Communications Session Border Controller	All	All	All	All
Application	Oracle	Communications Session Border Controller	7.2.0	-	All	All
Application	Oracle	Communications Session Border Controller	8.0.0	All	All	All
Application	Oracle	Communications Session Border Controller	All	All	All	All
Application	Oracle	Communications Session Border Controller	7.2.0	-	All	All
Application	Oracle	Communications Session Border Controller	8.0.0	All	All	All
Application	Oracle	Communications User Data Repository	All	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.0	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.1	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.0	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.1	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2	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	Linux	5	-	All	All
Operating System	Oracle	Linux	7	0	All	All
Operating System	Oracle	Linux	5	-	All	All
Operating System	Oracle	Linux	7	0	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Redhat	Virtualization	6.0	All	All	All
Application	Redhat	Virtualization	6.0	All	All	All

References

Reference

The glibc (Ghost) vulnerability: affected versions, recommended steps and workarounds

Security Advisory SA62813 - IBM Security Network Protection Multiple Vulnerabilities - Secunia

GNU glibc gethostbyname Function Buffer Overflow Vulnerability

www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt

Full Disclosure: SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series

About the security content of OS X Yosemite v10.10.4 and Security Update 2015-005 - Apple Support

Security Advisory SA62871 - IBM PureApplication System GNU C Library Buffer Overflow Vulnerability - Secunia

EMC Secure Remote Services GHOST / SQL Injection / Command Injection ≈ Packet Storm

oss-security - 21Nails: Multiple vulnerabilities in Exim

IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM Security Proventia Network Enterprise Scanner (CVE-2015-0235) - United S

Support / Security / Advisories // MDVSA-2015:039 | Mandriva

HPE Support document - HPE Support Center

Oracle Critical Patch Update - July 2016

Security Advisory SA62816 - F-Secure Messaging Security Gateway GNU C Library Buffer Overflow Vulnerability - Secunia

APPLE-SA-2015-10-21-4 OS X El Capitan 10.11.1 and Security Update 2015-007

IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM Security Virtual Server Protection for VMware (CVE-2015-0235) - United S

APPLE-SA-2015-09-30-3 OS X El Capitan 10.11

linux.oracle.com | ELSA-2015-0090 - glibc security update

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

IBM Security Bulletin: GNU C library (glibc) vulnerability affects QRadar SIEM, QRadar Risk Manager, and QRadar Vulnerability Manager (CV

Bugtraq: SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series

Red Hat Customer Portal

Vulnerabilities resolved in TRITON APX Version 8.0

Oracle Critical Patch Update - October 2015
oss-sec: GHOST gethostbyname() heap overflow in glibc (CVE-2015-0235)
Security Advisory SA62690 - Juniper Multiple Products GNU C Library Buffer Overflow Vulnerability - Secunia
Exim GHOST (glibc gethostbyname) Buffer Overflow ≈ Packet Storm
Moxa Command Injection / Cross Site Scripting / Vulnerable Software ≈ Packet Storm
IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM Workload Deployer (CVE-2015-0235) - United States
Oracle Critical Patch Update - July 2015
Security Advisory SA62691 - Blue Coat Multiple Products GNU C Library Buffer Overflow Vulnerability - Secunia
The Laws of Vulnerabilities: The GHOST Vulnerab... Qualys Community
IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM Security Access Manager for Web (CVE-2015-0235) - United States
Security Advisory SA62688 - Sophos Multiple Products GNU C Library Buffer Overflow Vulnerability - Secunia
Oracle Critical Patch Update - October 2016
Security Advisory SA62640 - IBM Security QRadar SIEM Multiple Vulnerabilities - Secunia
'[security bulletin] HPSB MU03330 rev.1 - HP Matrix Operating Environment (MOE) running glibc on Linux' - MARC
APPLE-SA-2015-06-30-2 OS X Yosemite v10.10.4 and Security Update 2015-005
Exim ESMTP GHOST Denial Of Service ≈ Packet Storm
72325
'[security bulletin] HPSB GN03285 rev.1 - HP Business Service Manager Virtual Appliance, Multiple Vul' - MARC
404 Not Found
Security Advisory SA62812 - IBM Security Access Manager for Web GNU C Library Buffer Overflow Vulnerability - Secunia
IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM Security Access Manager for Mobile (CVE-2015-0235) - United States
Security Advisory SA62870 - IBM Workload Deployer GNU C Library Buffer Overflow Vulnerability - Secunia
Security Advisory SA62517 - McAfee Multiple Products GNU C Library Buffer Overflow Vulnerability - Secunia
IBM Security Bulletin: GNU C library (glibc) vulnerability affects WebSphere Transformation Extender with Launcher Hypervisor Edition [for R]
'[security bulletin] HPSB GN03270 rev.1 - HP Operations Analytics, Remote Execution of Code' - MARC
Nexans FTTO GigaSwitch Outdated Components / Hardcoded Backdoor ≈ Packet Storm
Security Advisory SA62680 - Ubuntu update for eglibc - Secunia
Security Advisory SA62758 - IBM Security Access Manager for Mobile GNU C Library Buffer Overflow Vulnerability - Secunia
fsc-2015-1 F-Secure Labs
Home Blue Coat Systems, Inc.
IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM Security Network Protection (CVE-2015-0235) - United States
IBM Security Bulletin: GNU C library (glibc) vulnerability affects IBM PureApplication System (CVE-2015-0235) - United States
StruxureWare Data Center Operation Software Vulnerability Fixes - User Assistance for StruxureWare Data Center Operation 8 - Help Center
oss-sec: Qualys Security Advisory CVE-2015-0235 - GHOST: glibc gethostbyname buffer overflow
McAfee KnowledgeBase - McAfee Security Bulletin - GHOST Vulnerability

About the security content of OS X El Capitan 10.11.1, Security Update 2015-004 Yosemite, and Security Update 2015-007 Mavericks - Apple
Debian -- Security Information -- DSA-3142-1 eglibc
Juniper Networks - 2015-01 Out of Cycle Security Bulletin: GHOST glibc gethostbyname() buffer overflow vulnerability (CVE-2015-0235) - Know
Full Disclosure: Qualys Security Advisory CVE-2015-0235 - GHOST: glibc gethostbyname buffer overflow
Full Disclosure: SEC Consult SA-20210901-0 :: Multiple vulnerabilities in MOXA devices
Gentoo Security
Oracle Critical Patch Update - April 2015
Security Advisory SA62865 - IBM WebSphere Transformation Extender GNU C Library Buffer Overflow Vulnerability - Secunia
SecurityFocus
Security Advisory SA62879 - IBM Security Virtual Server Protection for VMware GNU C Library Buffer Overflow Vulnerability - Secunia
CPU Oct 2018
Security Advisory SA62692 - Cisco Multiple Products GNU C Library Buffer Overflow Vulnerability - Secunia
CVE-2015-0235 GNU C Library (glibc) Vulnerability in Multiple NetApp Products NetApp Product Security
Sophos products and the GHOST vulnerability affecting Linux Sophos Blog
Security Advisory SA62883 - IBM Proventia Network Enterprise Scanner GNU C Library Buffer Overflow Vulnerability - Secunia
Arista - Security Advisory 0009
About the security content of OS X El Capitan v10.11 - Apple Support
Security Advisory SA62698 - Oracle Linux update for glibc - Secunia
'[security bulletin] HPSBGN03247 rev.1 - HP IceWall SSO Dfw using glibc, Remote Execution of Arbitrary' - MARC
IBM Security Bulletin: Security Bulletin: GNU C library (glibc) vulnerability is fixed in IBM Security Access Manager for Enterprise Single Sign-On
Security Advisory SA62681 - SUSE update for glibc - Secunia
Security Advisory SA62715 - IBM Security Access Manager for Enterprise Single Sign-On GNU C Library Buffer Overflow Vulnerability - Secunia
Oracle Critical Patch Update - July 2017
'[security bulletin] HPSBHF03289 rev.1- HP ThinClient PCs running ThinPro Linux, Remote Code Execution' - MARC
Oracle Critical Patch Update - October 2017
Security Advisory SA62667 - Red Hat update for glibc - Secunia
linux.oracle.com ELSA-2015-0092 - glibc security update
Oracle Communications Applications Flaws Let Remote Users Gain Elevated Privileges and Partially Access Data, Modify Data, and Deny Se
cert-portal.siemens.com/productcert/pdf/ssa-994726.pdf
Oracle Critical Patch Update - January 2016
Full Disclosure: SEC Consult SA-20220615-0 :: Hardcoded Backdoor User and Outdated Software Components in Nexans FTTO GigaSwitch
WAGO 852 Industrial Managed Switch Series Code Execution / Hardcoded Credentials ≈ Packet Storm
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

591368 Eaton Power Xpert Gateway models buffer overflow Vulnerability (ETN-SB-2015-1002)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)