



CVE-2012-4412

Published on: 10/09/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:13 AM UTC

CVE-2012-4412

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Glibc](#) from [Gnu](#) contain the following vulnerability:

Integer overflow in string/strcoll_.l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buffer overflow.

CVE-2012-4412 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

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

[seclists.org](#)
[text/html](#)

[FULLDISC 20190612 SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series](#)

855385 – (CVE-2012-4412) CVE-2012-4412 glibc: strcoll() integer overflow leading to buffer overflow

[bugzilla.redhat.com](#)
[text/html](#)

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=855385](#)

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

[seclists.org](#)
[text/html](#)

[BUGTRAQ 20190613 SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series](#)

Support / Security / Advisories / / MDVSA-2013:284 | Mandriva

[www.mandriva.com](#)
[text/html](#)

[MANDRIVA MDVSA-2013:284](#)

oss-security - CVE Request -- glibc: strcoll() integer overflow leading to buffer overflow + another alloca() stack overflow issue (upstream #14547 && #14552)

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20130907 CVE Request -- glibc: strcoll\(\) integer overflow leading to buffer overflow + another alloca\(\) stack overflow issue](#)

(upstream #14547 && #14552)

Bug 14547 – strcoll integer / buffer overflow (CVE-2012-4412, CVE-2012-4424)

[Exploit](#)
[Patch](#)
[sourceware.org](#)
[text/html](#)

 **CONFIRM**
sourceware.org/bugzilla/show_bug.cgi?id=14547

About Secunia Research | Flexera

[secunia.com](#)
[Deprecated Link](#)
[text/plain](#)

 **SECUNIA 55113**

Support / Security / Advisories // MDVSA-2013:283 | Mandriva

[www.mandriva.com](#)
[text/html](#)

 **MANDRIVA MDVSA-2013:283**

Gentoo Security

[security.gentoo.org](#)
[text/html](#)

 **GENTOO GLSA-201503-04**

USN-1991-1: GNU C Library vulnerabilities | Ubuntu

[www.ubuntu.com](#)
[text/html](#)

 **UBUNTU USN-1991-1**

WAGO 852 Industrial Managed Switch Series Code Execution / Hardcoded Credentials ≈ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

 **MISC**
packetstormsecurity.com/files/153278/WAGO-852-Industrial-Managed-Switch-Series-Code-Execution-Hardcoded-Credentials.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.9	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	2.12.1	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	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.9	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	2.12.1	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	All	All	All	All
		cpe:2.3:a:gnu:glibc:2.0:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.2:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.3:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.4:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.5:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.6:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.1.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.1.1.6:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.1.2:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.1.3:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.1.9:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.10.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.11:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.11.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.11.2:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.11.3:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.12.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.12.2:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.13:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.14:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.14.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.15:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.16:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.1:*:*:*:*:*:*:				
		cpe:2.3:a:gnu:glibc:2.0.2:*:*:*:*:*:*:				

cpe:2.3:a:gnu:glibc:2.0.3:*****:
cpe:2.3:a:gnu:glibc:2.0.4:*****:
cpe:2.3:a:gnu:glibc:2.0.5:*****:
cpe:2.3:a:gnu:glibc:2.0.6:*****:
cpe:2.3:a:gnu:glibc:2.1:*****:
cpe:2.3:a:gnu:glibc:2.1.1:*****:
cpe:2.3:a:gnu:glibc:2.1.1.6:*****:
cpe:2.3:a:gnu:glibc:2.1.2:*****:
cpe:2.3:a:gnu:glibc:2.1.3:*****:
cpe:2.3:a:gnu:glibc:2.1.9:*****:
cpe:2.3:a:gnu:glibc:2.10.1:*****:
cpe:2.3:a:gnu:glibc:2.11:*****:
cpe:2.3:a:gnu:glibc:2.11.1:*****:
cpe:2.3:a:gnu:glibc:2.11.2:*****:
cpe:2.3:a:gnu:glibc:2.11.3:*****:
cpe:2.3:a:gnu:glibc:2.12.1:*****:
cpe:2.3:a:gnu:glibc:2.12.2:*****:
cpe:2.3:a:gnu:glibc:2.13:*****:
cpe:2.3:a:gnu:glibc:2.14:*****:
cpe:2.3:a:gnu:glibc:2.14.1:*****:
cpe:2.3:a:gnu:glibc:2.15:*****:
cpe:2.3:a:gnu:glibc:2.16:*****:
cpe:2.3:a:gnu:glibc:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)