



CVE-2004-1455

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

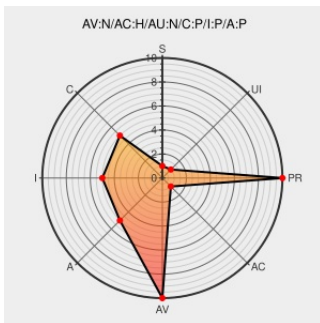
CVE-2004-1455

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Xine-lib](#) from [Xine](#) contain the following vulnerability:

Stack-based buffer overflow in Xine-lib-rc5 in xine-lib 1_rc5-r2 and earlier allows remote attackers to execute arbitrary code via crafted playlists that result in a long vcd:// URL.

CVE-2004-1455 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Gentoo Linux Documentation -- xine-lib: VCD MRL buffer overflow

[Patch](#)
[www.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-200408-18](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF xine-vcd-identifier-bo\(16930\)](#)

Secunia - Advisories - Xine "vcd:" Input Source Buffer Overflow Vulnerability

[web.archive.org](#)
[text/html](#)

[SECUNIA 12194](#)

Xine-Lib Remote Buffer Overflow Vulnerability

[Exploit](#)
[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 10890](#)

Nothing found for Advisories 6

[open-security.org](#)
[text/x-c](#)

[MISC open-security.org/advisories/6](#)

'Open Security Group Advisory #6' - MARC

[marc.info](#)[text/html](#) [BUGTRAQ 20040817 Open Security Group Advisory #6](#)

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	Xine	Xine-lib	1_beta1	All	All	All
Application	Xine	Xine-lib	1_beta10	All	All	All
Application	Xine	Xine-lib	1_beta11	All	All	All
Application	Xine	Xine-lib	1_beta2	All	All	All
Application	Xine	Xine-lib	1_beta3	All	All	All
Application	Xine	Xine-lib	1_beta4	All	All	All
Application	Xine	Xine-lib	1_beta5	All	All	All
Application	Xine	Xine-lib	1_beta6	All	All	All
Application	Xine	Xine-lib	1_beta7	All	All	All
Application	Xine	Xine-lib	1_beta8	All	All	All
Application	Xine	Xine-lib	1_beta9	All	All	All
Application	Xine	Xine-lib	1_rc2	All	All	All
Application	Xine	Xine-lib	1_rc3a	All	All	All
Application	Xine	Xine-lib	1_rc3b	All	All	All
Application	Xine	Xine-lib	1_rc3c	All	All	All
Application	Xine	Xine-lib	1_rc4	All	All	All
Application	Xine	Xine-lib	1_rc5	All	All	All
Application	Xine	Xine-lib	1_rc5_r2	All	All	All
Application	Xine	Xine-lib	1_beta1	All	All	All
Application	Xine	Xine-lib	1_beta10	All	All	All
Application	Xine	Xine-lib	1_beta11	All	All	All
Application	Xine	Xine-lib	1_beta2	All	All	All
Application	Xine	Xine-lib	1_beta3	All	All	All
Application	Xine	Xine-lib	1_beta4	All	All	All
Application	Xine	Xine-lib	1_beta5	All	All	All

Application	Xine	Xine-lib	1_beta6	All	All	All
Application	Xine	Xine-lib	1_beta7	All	All	All
Application	Xine	Xine-lib	1_beta8	All	All	All
Application	Xine	Xine-lib	1_beta9	All	All	All
Application	Xine	Xine-lib	1_rc2	All	All	All
Application	Xine	Xine-lib	1_rc3a	All	All	All
Application	Xine	Xine-lib	1_rc3b	All	All	All
Application	Xine	Xine-lib	1_rc3c	All	All	All
Application	Xine	Xine-lib	1_rc4	All	All	All
Application	Xine	Xine-lib	1_rc5	All	All	All
Application	Xine	Xine-lib	1_rc5_r2	All	All	All
cpe:2.3:a:xine:xine-lib:1_beta1:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta10:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta11:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta2:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta3:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta4:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta5:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta6:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta7:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta8:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta9:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc2:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc3a:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc3b:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc3c:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc4:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc5:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_rc5_r2:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta1:****:*:*:						
cpe:2.3:a:xine:xine-lib:1_beta10:****:*:*:						

cpe:2.3:a:xine:xine-lib:1_beta11:*****:
cpe:2.3:a:xine:xine-lib:1_beta2:*****:
cpe:2.3:a:xine:xine-lib:1_beta3:*****:
cpe:2.3:a:xine:xine-lib:1_beta4:*****:
cpe:2.3:a:xine:xine-lib:1_beta5:*****:
cpe:2.3:a:xine:xine-lib:1_beta6:*****:
cpe:2.3:a:xine:xine-lib:1_beta7:*****:
cpe:2.3:a:xine:xine-lib:1_beta8:*****:
cpe:2.3:a:xine:xine-lib:1_beta9:*****:
cpe:2.3:a:xine:xine-lib:1_rc2:*****:
cpe:2.3:a:xine:xine-lib:1_rc3a:*****:
cpe:2.3:a:xine:xine-lib:1_rc3b:*****:
cpe:2.3:a:xine:xine-lib:1_rc3c:*****:
cpe:2.3:a:xine:xine-lib:1_rc4:*****:
cpe:2.3:a:xine:xine-lib:1_rc5:*****:
cpe:2.3:a:xine:xine-lib:1_rc5_r2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)