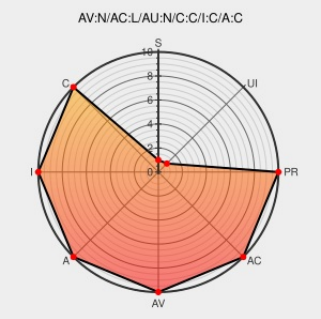
CVE-2004-0964

Published on: 10/20/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:12 PM UTC

CVE-2004-0964

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

Buffer overflow in Zinf 2.2.1 on Windows, and other older versions for Linux, allows remote attackers or local users to execute arbitrary code via certain values in a .pls file.

CVE-2004-0964 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF zinf-pls-bo(17491)
Debian -- Security Information -- DSA-587-1 freeamp	Patch, Vendor Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-587
Zinf Malformed Playlist File Remote Buffer Overflow Vulnerability	Exploit, Patch, Vendor Advisory, cve.report (archive), text/html	BID 11248
Zinf Audio Player v2.2.1 PLS File Buffer Overflow Vulnerability (DEP BYPASS) - CXSecurity.com	securityreason.com, text/html	SREASON 8341

'Re: Buffer overflow in Zinf 2.2.1 for Win32+exploit' - MARC	marc.info text/x-c	BUGTRAQ 20040927 Re: Buffer overflow in Zinf 2.2.1 for Win32+exploit
'Buffer overflow in Zinf 2.2.1 for Win32' - MARC	marc.info text/html	BUGTRAQ 20040924 Buffer overflow in Zinf 2.2.1 for Win32
Secunia - Advisories - Zinf Playlist Handling Buffer Overflow Vulnerability	web.archive.org text/html	SECUNIA 12656

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.0	All	alpha	All
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-32	All
Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating System	Debian	Debian Linux	3.0	All	mips	All
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Operating System	Debian	Debian Linux	3.0	All	alpha	All
Operating System	Debian	Debian Linux	3.0	All	arm	All
Operating System	Debian	Debian Linux	3.0	All	hppa	All
Operating System	Debian	Debian Linux	3.0	All	ia-32	All

System						
Operating System	Debian	Debian Linux	3.0	All	ia-64	All
Operating System	Debian	Debian Linux	3.0	All	m68k	All
Operating System	Debian	Debian Linux	3.0	All	mips	All
Operating System	Debian	Debian Linux	3.0	All	mipsel	All
Operating System	Debian	Debian Linux	3.0	All	ppc	All
Operating System	Debian	Debian Linux	3.0	All	s-390	All
Operating System	Debian	Debian Linux	3.0	All	sparc	All
Application	Zinf	Zinf	2.2.1	All	All	All
Application	Zinf	Zinf	2.2.1	All	All	All

cpe:2.3:o:debian:debian_linux:3.0:*:alpha:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:arm:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:hppa:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:ia-32:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:ia-64:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:m68k:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:mips:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:mipsel:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:ppc:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:s-390:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:sparc:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:alpha:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:arm:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:hppa:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:ia-32:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:ia-64:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:m68k:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:mips:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:mipsel:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:ppc:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:s-390:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.0:*:sparc:*:*:*:*:*:

cpe:2.3:a:zinf:zinf:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:zinf:zinf:2.2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→