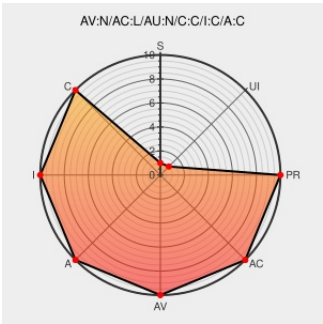
CVE-2004-0994

Published on: 12/15/2004 12:00:00 AM UTC

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

CVE-2004-0994

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



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

Multiple integer overflows in xzgv 0.8 and earlier allow remote attackers to execute arbitrary code via images with large width and height values, which trigger a heap-based buffer overflow, as demonstrated in the read_prf_file function in readprf.c. NOTE: CVE-2004-0994 and CVE-2004-1095 identify sets of bugs that only partially overlap, despite having the same developer. Therefore, they should be regarded as distinct.

CVE-2004-0994 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
Debian -- Security Information -- DSA-614-1 xzgv	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-614
	rus.members.beeb.net, text/x-diff, Inactive Link, Not Archived	CONFIRM rus.members.beeb.net/xzgv-0.8-integer-overflow-fix.diff
'iDEFENSE Security Advisory 12.13.04 - Multiple Vendor xzgv PRF Parsing Integer Overflow Vulnerabilit' - MARC	marc.info, text/html	IDEFENSE 20041213 Multiple Vendor xzgv PRF Parsing Integer Overflow Vulnerability
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF xzgv-readprffile-bo(18454)

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
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
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

System						
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	Zgv	Xzgv Image Viewer	0.6	All	All	All
Application	Zgv	Xzgv Image Viewer	0.7	All	All	All
Application	Zgv	Xzgv Image Viewer	0.8	All	All	All
Application	Zgv	Xzgv Image Viewer	0.6	All	All	All
Application	Zgv	Xzgv Image Viewer	0.7	All	All	All
Application	Zgv	Xzgv Image Viewer	0.8	All	All	All
Application	Zgv	Zgv Image Viewer	5.5	All	All	All
Application	Zgv	Zgv Image Viewer	5.6	All	All	All
Application	Zgv	Zgv Image Viewer	5.7	All	All	All
Application	Zgv	Zgv Image Viewer	5.8	All	All	All
Application	Zgv	Zgv Image Viewer	5.5	All	All	All
Application	Zgv	Zgv Image Viewer	5.6	All	All	All
Application	Zgv	Zgv Image Viewer	5.7	All	All	All
Application	Zgv	Zgv Image Viewer	5.8	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:zgv:xzgv_image_viewer:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:xzgv_image_viewer:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:xzgv_image_viewer:0.8:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:xzgv_image_viewer:0.6:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:xzgv_image_viewer:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:xzgv_image_viewer:0.8:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.6:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.7:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.8:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.6:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.7:*:*:*:*:*:*:*:

cpe:2.3:a:zgv:zgv_image_viewer:5.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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