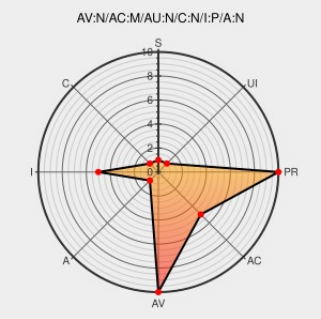
CVE-2003-0615

Published on: 08/01/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-0615

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



Certain versions of Cgi.pm from Cgi.pm contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in start_form() of CGI.pm allows remote attackers to insert web script via a URL that is fed into the form's action parameter.

CVE-2003-0615 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
'[OpenPKG-SA-2003.036] OpenPKG Security Advisory (perl-www)' - MARC	marc.info text/html	BUGTRAQ 20030806 [OpenPKG-SA-2003.036] OpenPKG Security Advisory (perl-www)
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF cgi-startform-xss(12669)
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC N-155
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:256
SecurityTracker.com Archives - CGI.pm Library Input Validation Flaw Permits Remote Cross-Site Scripting Attacks	securitytracker.com text/html	SECTRACK 1007234

Advisories - Mandriva	wwwnew.mandriva.com text/html	MANDRAKE MDKSA-2003:084
CGI.pm Start_Form Cross-Site Scripting Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 8231
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:307
'CGI.pm vulnerable to Cross-site Scripting' - MARC	marc.info text/html	BUGTRAQ 20030720 CGI.pm vulnerable to Cross-site Scripting
#101426: Security Vulnerabilities in "Safe.pm" and "CGI.pm" Perl Modules (formerly Document ID: 57473)	web.archive.org text/html Inactive Link Not Archived	SUNALERT 101426
CERT/CC Vulnerability Note VU#246409	US Government Resource www.kb.cert.org text/html	CERT-VN VU#246409
Secunia - Advisories - Sun Solaris Perl Modules Two Vulnerabilities	web.archive.org text/html	SECUNIA 13638
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:470
Debian -- Security Information -- DSA-371-1 perl	www.debian.org Depreciated Link text/html	DEBIAN DSA-371
'[Full-Disclosure] CGI.pm vulnerable to Cross-site Scripting.' - MARC	marc.info text/html	FULLDISC 20030720 CGI.pm vulnerable to Cross-site Scripting.
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLA-2003:713

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cgi.pm	Cgi.pm	2.73	All	All	All
Application	Cgi.pm	Cgi.pm	2.74	All	All	All
Application	Cgi.pm	Cgi.pm	2.75	All	All	All
Application	Cgi.pm	Cgi.pm	2.751	All	All	All
Application	Cgi.pm	Cgi.pm	2.753	All	All	All
Application	Cgi.pm	Cgi.pm	2.76	All	All	All
Application	Cgi.pm	Cgi.pm	2.78	All	All	All
Application	Cgi.pm	Cgi.pm	2.79	All	All	All

Application	Cgi.pm	Cgi.pm	2.93	All	All	All
Application	Cgi.pm	Cgi.pm	2.73	All	All	All
Application	Cgi.pm	Cgi.pm	2.74	All	All	All
Application	Cgi.pm	Cgi.pm	2.75	All	All	All
Application	Cgi.pm	Cgi.pm	2.751	All	All	All
Application	Cgi.pm	Cgi.pm	2.753	All	All	All
Application	Cgi.pm	Cgi.pm	2.76	All	All	All
Application	Cgi.pm	Cgi.pm	2.78	All	All	All
Application	Cgi.pm	Cgi.pm	2.79	All	All	All
Application	Cgi.pm	Cgi.pm	2.93	All	All	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
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	Debian	Debian Linux	3.0	All	m68k	All

System						
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	Openpkg	Openpkg	1.2	All	All	All
Application	Openpkg	Openpkg	1.3	All	All	All
Application	Openpkg	Openpkg	current	All	All	All
Application	Openpkg	Openpkg	1.2	All	All	All
Application	Openpkg	Openpkg	1.3	All	All	All
Application	Openpkg	Openpkg	current	All	All	All

cpe:2.3:a:cgi.pm:cgi.pm:2.73:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.74:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.75:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.751:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.753:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.76:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.78:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.79:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.93:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.73:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.74:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.75:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.751:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.753:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.76:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.78:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.79:*:*:*:*:*:*:*:

cpe:2.3:a:cgi.pm:cgi.pm:2.93:*:*:*:*:*:*:*:

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:openpkg:openpkg:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:openpkg:openpkg:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:openpkg:openpkg:current:*:*:*:*:*:*:*:

cpe:2.3:a:openpkg:openpkg:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:openpkg:openpkg:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:openpkg:openpkg:current:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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