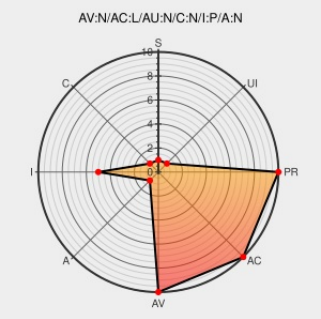
CVE-2003-1365

Published on: 12/31/2003 05:00:00 AM UTC

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

CVE-2003-1365

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



Certain versions of Cgi Lite from Perl contain the following vulnerability:

The escape_dangerous_chars function in CGI::Lite 2.0 and earlier does not correctly remove special characters including (1) "\" (backslash), (2) "?", (3) "~" (tilde), (4) "^" (carat), (5) newline, or (6) carriage return, which could allow remote attackers to read or write arbitrary files, or execute arbitrary commands, in shell scripts that rely on CGI::Lite to filter such dangerous inputs.

CVE-2003-1365 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Neohapsis Archives - VulnWatch - [VulnWatch] Security bug in CGI::Lite::escape_dangerous_chars() function - From rfg_at_monkeys.com	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	VULNWATCH 20030211 Security bug in CGI::Lite::escape_dangerous_chars() function
Journal of cbrooks (3267)	web.archive.org, text/html, Inactive Link, Not Archived	MISC use.perl.org/~cbrooks/journal/10542
CGI Lite Perl Module Metacharacter Input Validation Vulnerability	cve.report (archive), text/html	BID 6833
Security bug in CGI::Lite::escape_dangerous_chars() function - CXSecurity.com	securityreason.com, text/html	SREASON 3237

search.cpan.org: CGI::Lite - Process and decode WWW forms and cookies	Exploit search.cpan.org text/html	CONFIRM search.cpan.org/~smylers/CGI-Lite-2.02/Lite.pm
SecurityFocus HOME Mailing List: BugTraq	Exploit www.securityfocus.com text/html	BUGTRAQ 20030211 Security bug in CGI::Lite::escape_dangerous_chars() function
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF cgilite-shell-command-execution(11308)

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	Perl	Cgi Lite	2.0	All	All	All
Application	Perl	Cgi Lite	2.0	All	All	All

cpe:2.3:a:perl:cgi_lite:2.0:*:*:*:*:*:*:*

cpe:2.3:a:perl:cgi_lite:2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→