



CVE-2011-2766

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-2766
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-23 10:55:00 UTC
Updated	2020-12-08 15:24:00 UTC
Description	The FCGI (aka Fast CGI) module 0.70 through 0.73 for Perl, as used by CGI::Fast, uses environment variable values from

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Fast Cgi Project	Fast Cgi	All	All	All	All

References

Reference
openSUSE-SU-2012:0036
#607479 - libfcgi-perl: [CVE-2011-2766] After reloading some environment vars become constants, that will be used if not overruled by the he
oss-security - Re: CVE Request -- libfcgi-perl / perl-FCGI: Certain environment variables shared between first and subsequent HTTP requests
oss-security - CVE Request -- libfcgi-perl / perl-FCGI: Certain environment variables shared between first and subsequent HTTP requests
Bug #68380 for FCGI: FCGI-0.70 to 0.72 with perl5.12: CGI.pm receives CGI variables from previous requests
IBM X-Force Exchange
Support / Security / Advisories / / MDVSA-2012:001 Mandriva

Perl Fast CGI Module CGI Variables Authentication Security Bypass Vulnerability
openSUSE-SU-2012:0004
Debian -- Security Information -- DSA-2327-1 libfcgi-perl
Bug 736604 – CVE-2011-2766 perl-FCGI, fcgi: Certain environment variables shared between first and subsequent HTTP requests
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
Legacy QID Mappings
900136 CBL-Mariner Linux Security Update for perl 5.30.3

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)