CVE-2011-3607

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-3607
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-11-08 11:55:05 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x throu

Risk And Classification

Primary CVSS: v2.0 4.4 from nvd@nist.gov

AV:L/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.0	All	All	All

Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	All	All
Application	Apache	Http Server	2.0.34	beta	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	All	All	All
Application	Apache	Http Server	2.0.56	All	All	All
Application	Apache	Http Server	2.0.57	All	All	All
Application	Apache	Http Server	2.0.58	All	All	All
Application	Apache	Http Server	2.0.59	All	All	All
Application	Apache	Http Server	2.0.60	All	All	All
Application	Apache	Http Server	2.0.61	All	All	All
Application	Apache	Http Server	2.0.63	All	All	All
Application	Apache	Http Server	2.0.64	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.2.0	All	All	All

Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.10	All	All	All
Application	Apache	Http Server	2.2.11	All	All	All
Application	Apache	Http Server	2.2.12	All	All	All
Application	Apache	Http Server	2.2.13	All	All	All
Application	Apache	Http Server	2.2.14	All	All	All
Application	Apache	Http Server	2.2.15	All	All	All
Application	Apache	Http Server	2.2.16	All	All	All
Application	Apache	Http Server	2.2.18	All	All	All
Application	Apache	Http Server	2.2.19	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.4	All	All	All
Application	Apache	Http Server	2.2.6	All	All	All
Application	Apache	Http Server	2.2.8	All	All	All
Application	Apache	Http Server	2.2.9	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Pony Mail!
Apache HTTP Server 'ap_pregsub()' Function Local Privilege Escalation Vulnerability
IBM X-Force Exchange
Oracle Critical Patch Update - July 2012
HPSBMU02786 SSRT100877 rev.2 - HP System Management Homepage (SMH) Running on Linux, Windows, and VMware ESX, Remote Ur
Pony Mail!
Pony Mail!
Debian -- Security Information -- DSA-2405-1 apache2
Security Alerts - Secunia
Pony Mail!
Pony Mail!

Pony Mail!

Support / Security / Advisories / / MDVSA-2012:003 | Mandriva

Red Hat Customer Portal

Pony Mail!

NEOHAPSIS - Peace of Mind Through Integrity and Insight

Pony Mail!

www.osvdb.org/76744

Pony Mail!

Pony Mail!

'[security bulletin] HPSBMU02748 SSRT100772 rev.1 - HP OpenView Network Node Manager (OV NNM) Running' - MARC

Pony Mail!

Pony Mail!

Pony Mail!

Apache .htaccess File Integer Overflow Lets Local Users Execute Arbitrary Code - SecurityTracker

access.redhat.com

Pony Mail!

About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004

Bug 750935 – CVE-2011-4415 httpd: SetEnvIf resource exhaustion

About Secunia Research | Flexera

Pony Mail!

Exploitation of Integer Overflow in Apache 2.2.19 mod-setenvif

Integer Overflow in Apache ap_pregsub via mod-setenvif

This page provides Security Information. - Fujitsu Global

Support / Security / Advisories / / MDVSA-2013:150 | Mandriva

Pony Mail!

Bug #811422 “Exploitable integer overflow on x86 in mod SetEnvIf...” : Bugs : “apache2” package : Ubuntu

Pony Mail!

access.redhat.com

'[security bulletin] HPSBOV02822 SSRT100966 rev.1 - HP Secure Web Server (SWS) for OpenVMS, Remote De' - MARC

Pony Mail!

'[security bulletin] HPSBUX02761 SSRT100823 rev.1 - HP-UX Running Apache, Remote Denial of Service (D' - MARC

Pony Mail!

Pony Mail!

Oracle Critical Patch Update - January 2015

Pony Mail!

Pony Mail!
APPLE-SA-2012-09-19-2 OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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