OWASP
Open Web Application
Security Project

CVE

Lo bueno, Lo malo y Lo feo

Algunos datos importantes

74.991 Vulnerabilidades registradas como CVE

Fuente: Howlermonkey.io

El 30 % de las vulnerabilidades registradas son graves

Fuente: Howlermonkey.io

En el 2016 Se han registrado 1497 vulnerabilidades

Fuente: Howlermonkey.io

IDENTIFICADOR CVE (CVE-id)

Search by CVE ID

CVE-2008-1447 Search

CVE-2008-1447

CVSS: 5.0
CVSS Time: 2008-07-09T11:22:00.000-04:00
CWE: CWE-310
Published: 2008-07-08T19:41:00.000-04:00
Updated: 2015-03-16T21:59:27.210-04:00
Summary: The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2) Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via a birthday attack that uses in-bailiwick referrals to conduct cache poisoning against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability" or "the Kaminsky bug."

ACCESS

Vector: NETWORK **Authentication:** NONE **Complexity:** LOW

IMPACT

Availability: PARTIAL **Confidentiality:** NONE **Integrity:** PARTIAL

Search by CVE ID

CVE-2010-3333 Search

REFERENCES

http://www.us-cert.gov/cas/techalerts/TA10-313A.html
http://www.microsoft.com/technet/security/Bulletin/MS10-087.mspx
http://www.vupen.com/english/advisories/2010/2923
http://www.securitytracker.com/id?1024705
http://www.securityfocus.com/bid/44652
http://securityreason.com/securityalert/8293
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=880

BID ID: 44652

Exploit DB ID: 17474
Exploit DB Script: platforms/windows/local/17474.txt

MS ID: MS10-087
MS Title: MS10-087

MSF ID: ms10_087_rtf_pfragments_bof.rb
MSF Script Name: MS10-087 Microsoft Word RTF pFragments Stack Buffer Overflow (File Format)
MSF Script File: metasploit-framework/modules/exploits/windows/fileformat/ms10_087_rtf_pfragments_bof.rb

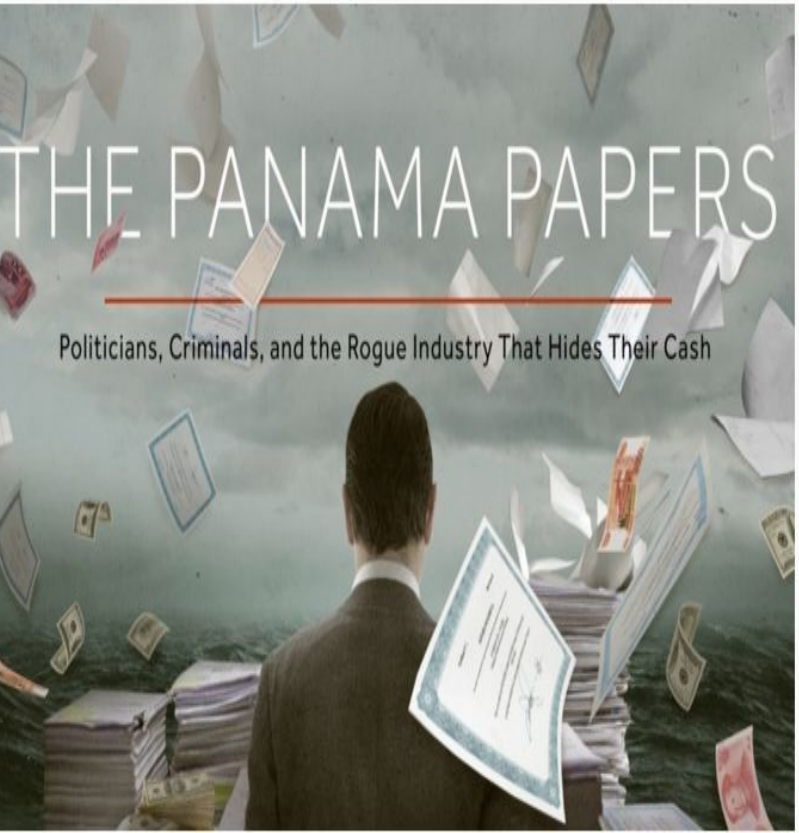

El Bueno


El Malo


El Feo

Un plugin de WordPress y un Drupal antiguo, causantes de la filtración de los Papeles de Panamá

f 2293



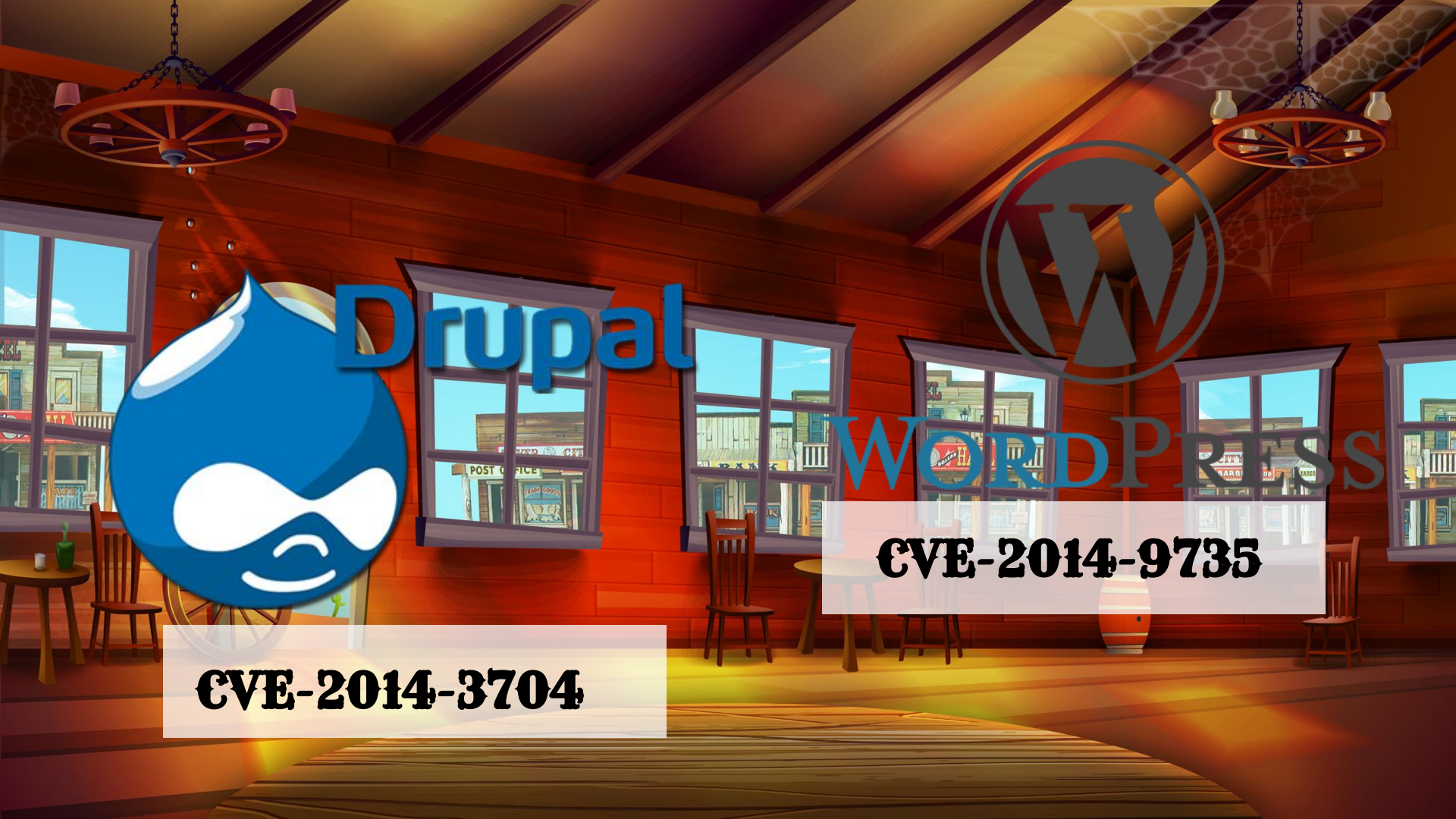
Panama Papers: Email Hackable via WordPress, Docs Hackable via Drupal

This entry was posted in General Security, WordPress Security on April 8, 2016 by mark 31 Replies

The Mossack Fonseca (MF) data breach, aka Panama Papers, is the largest data breach to journalists in history and includes over 4.8 million emails. Yesterday we broke the story that MF was running WordPress with a vulnerable version of Revolution Slider and the WordPress server was on the same network as their email servers when the breach occurred....read more

Mossack Fonseca Breach – WordPress Revolution Slider Plugin Possible Cause

This entry was posted in General Security, WordPress Security on April 7, 2016 by mark 54 Replies


Drupal
WORDPRESS
CVE-2014-9735
CVE-2014-3704

Ventajas del CVE

---> Es una base para la evaluación de las vulnerabilidades

---> Es un estándar muy adaptado para diferenciar vulnerabilidades

---> Posibilidad de monitorear los contenidos de las vulnerabilidades

---> Realiza un proceso de actualización continua de las vulnerabilidades registradas

OWASP
Open Web Application Security Project

FIN

Josmell Chavarri
josmell.chavarri@owasp.org
Twitter: @josmell24