Security Newsletter

25 February 2019

Subscribe to this newsletter

Drupal Fixes “Highly Critical” Vulnerability

Administrators of websites running the Drupal content management software (CMS) are urged to take immediate action to mitigate a newly discovered a vulnerability that can lead to remote execution of PHP code under specific circumstances.

If an update to the latest version o the CMS is not possible at the moment, the Drupal team offers alternative action to temporarily mitigate potential risk: disable all web services modules or configure the web server to reject PUT/PATCH/POST requests to web services resources.

Drupal is the world's third most popular content management system, commanding 4 percent market share, after Joomla at 5 percent and CMS heavyweight WordPress, which owns 60 percent of the market, according to W3Techs.com. It is worth noting that releases prior to 8.5.x are have reached end-of-life and no longer receive security updates.

Read More on BleepingComputer

Even More on BankInfoSecurity

2.7M recorded medical calls from 1177 Swedish Healthcare, audio files left unprotected on web

Every call made to 1177 Swedish Healthcare Guide service since 2013, and answered by the subcontractor Medicall, was stored as WAV or MP3 audio files on a server that had no encryption or authentication protection.

IDG's Computer Sweden revealed that 2.7 million recorded calls made to the 1177 national health service were left completely unprotected on a server. Every call made to 1177 since 2013, and answered by the subcontractor Medicall, was stored as WAV or MP3 audio files on a server that had no encryption or authentication protection. That adds up to "170,000 hours of sensitive phone calls with symptoms, etc.," which anyone with the right IP address could have accessed. Some of the audio files, which were marked with the callers' telephone numbers, included the Social Security numbers of children and adults and specific health-related symptoms.

Tommy Ekstrom, CEO of Voice Integrate Nordic, told IDG, "This is catastrophic, It's sensitive data. We had no idea that it was like this. We will, of course, review our systems and check out what may have happened."

Read More on CSOOnline

Original Source (Swedish)

More #News

- How to Hack Facebook Accounts? Just Ask Your Targets to Open a Link
- A third of all Chrome extensions request access to user data on any site
- NoRelationship phishing attack dances around Microsoft Office 365 email filters

- The Windows 10 security guide: How to safeguard your business
- Microsoft Edge Secret Whitelist Allows Facebook to Autorun Flash
- Why Cybersecurity Burnout Is Real (and What to Do About It)
- WhatsApp Flaw Could Enable iOS Message Snooping
- Password managers leaking data in memory, but you should still use one
- Warning: Critical WinRAR Flaw Affects All Versions Released In Last 19 Years
- Blockchain and Trust
- Criminals, Nation-States Keep Hijacking BGP and DNS
- LPG Gas Company Leaked Details, Aadhaar Numbers of 6.7 Million Indian Customers
- Here Come the Malicious USB Cables
- Google working on new Chrome security feature to 'obliterate DOM XSS'
- Fake Google reCAPTCHA used to hide Android banking malware

#Patch Time!

- Windows Servers Vulnerable to IIS Resource Exhaustion DoS Attacks
- Critical Flaw Uncovered In WordPress That Remained Unpatched for 6 Years
- Adobe Patches Critical Information Disclosure Flaw in Reader, Again
- Cisco Patches High Severity Flaws in HyperFlex, Prime Infrastructure
- Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003

#Tech and #Tools

- Easy & Flexible Alerting With ElasticSearch https://elastalert.readthedocs.org
- Kali Linux 2019.1 Released with Metasploit 5.0
- FIRST CSIRT Framework
- Red teaming on AWS with GuardDuty
- Putting Sysmon v9.0 AND/OR Grouping Logic to the Test
- Extracting a 19 Year Old Code Execution from WinRAR
- Password Managers: Under the Hood of Secrets Management
- MikroTik Firewall & NAT Bypass
- Our publications of the Swiss E-Voting Public Intrusion Test (PIT)
- Breaking out of Docker via runC – Explaining CVE-2019-5736
- Abusing autoresponders and email bounces
- Hacking Jenkins Part 1 - Play with Dynamic Routing (part 2)
- Venom - A Multi-hop Proxy for Penetration Testers
- WordPress 5.0.0 Remote Code Execution - technical writeup
- Red Team Techniques: Gaining access on an external engagement through spear-phishing
- How To Make The Most Out Of Security Conferences
- How to Test Bro-Sysmon

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us