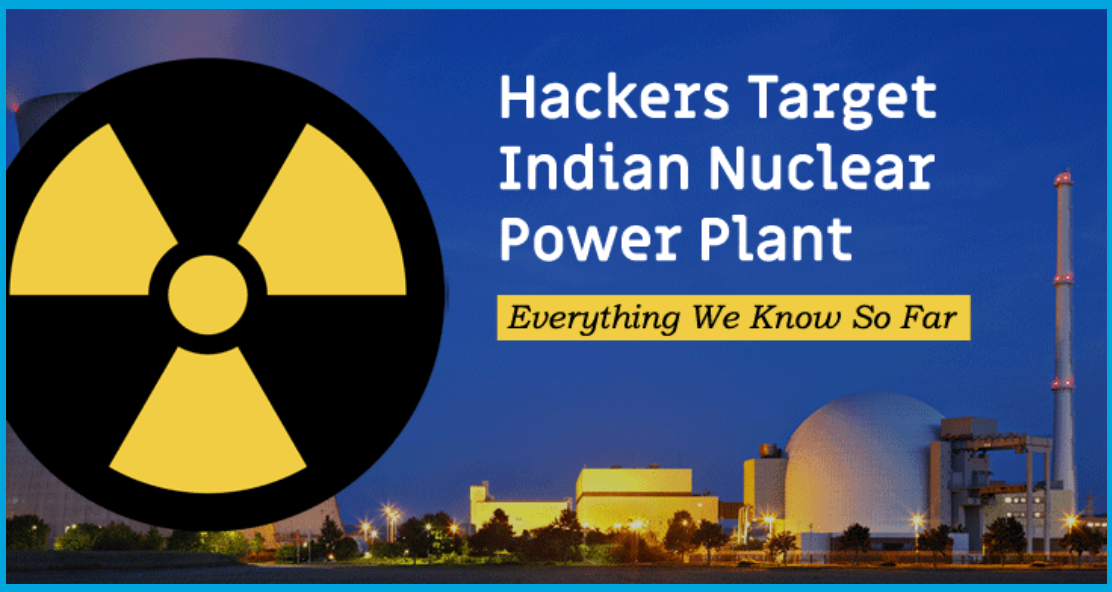
Security Newsletter

4 November 2019

Subscribe to this newsletter

Hackers Target Indian Nuclear Power Plant – What We Know So Far



Due to some experts commentary on social media even after lack of information about the event and overreactions by many, the incident received factually incorrect coverage widely suggesting a piece of malware has compromised "mission-critical systems" at the Kudankulam Nuclear Power Plant. That's not what happened. The attack only infected a system that was not connected to any critical controls in the nuclear facility.

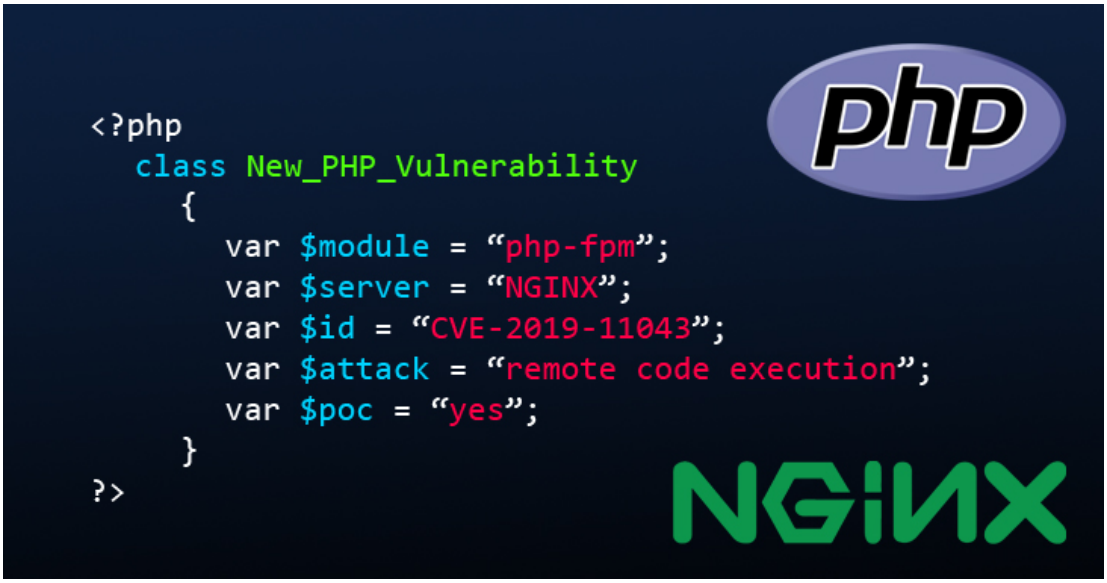
The story started when Indian security researcher Pukhraj Singh tweeted that he informed Indian authorities a few months ago about an information-stealing malware, dubbed Dtrack. According to a previous report published by researchers at Kaspersky, Dtrack is a remote access Trojan (RAT) intended to spy on its victims and install various malicious modules on the targeted computers, including: keylogger, browser history stealer, functions that collect host IP address, etc.

Immediately after Pukhraj's tweet, many Twitter users and Indian opposition politicians, including Congress MP Shashi Tharoor, demanded an explanation from the Indian Government about the alleged cyberattack — which it never disclosed to the public. In response to the initial media reports, the Nuclear Power Corporation of India (NPCIL), a government-owned entity, on Tuesday released an official statement, denying any cyber attack on the control system of the nuclear power plant. Though North Korean hackers developed the malware, the Indian Government has not yet attributed the attack to any group or country.

Read More on TheHackerNews

Even More on ZDNet

New PHP Flaw Could Let Attackers Hack Sites Running On Nginx Servers



If you're running any PHP based website on NGINX server and have PHP-FPM feature enabled for better performance, then beware of a newly disclosed vulnerability that could allow unauthorized attackers to hack your website server remotely. PHP-FPM is an alternative PHP FastCGI implementation that offers advanced and highly-efficient processing for scripts written in PHP programming language.

The vulnerability, tracked as CVE-2019-11043, affects websites with certain configurations of PHP-FPM that is reportedly not uncommon in the wild and could be exploited easily as a proof-of-concept (PoC) exploit for the flaw has already been released publicly. Though the publicly released PoC exploit is designed to specifically target vulnerable servers running PHP 7+ versions, the PHP-FPM underflow bug also affects earlier PHP versions and could be weaponized in a different way.

A Patch for this vulnerability was released just yesterday, almost a month after researchers reported it to the PHP developer team. Since the PoC exploit is already available and the patch released just yesterday, it's likely possible that hackers might have already started scanning the Internet in search for vulnerable websites. So, users are strongly advised to update PHP to the latest PHP 7.3.11 and PHP 7.2.24. Just do it, even if you are not using the vulnerable configuration.

Read More on TheHackerNews

Even More on ZDNet

Researchers find hole in EU-wide identity system

A flaw in a cross-border EU electronic identity system could have allowed anyone to impersonate someone else, a security consulting company has warned. SEC Consult issued an advisory warning people of the flaw this week. It demonstrated the problem in the electronic identification, authentication and trust services (eIDAS) system by authenticating as 16th-century German writer, Johann Wolfgang von Goethe.

eIDAS came about because of a 2014 EU regulation that laid out the rules for electronic identification in Europe. The regulation, which came into effect in 2016, made it compulsory for EU countries to identify each other's electronic IDs by the middle of last year. It covered a range of identification assets like electronic signatures and website authentication. The problem is that there's a flaw in the software used to manage this cross-border identification process, known as eIDAS-Node. Each country has to run a copy of this software to connect its own national identity management systems to others in the EU, creating a cross-border ID gateway. Using this gateway, citizens in the UK, say, could identify themselves to use electronic services in Germany, such as enrolling in a university or opening a bank account.

Luckily, the EU fixed the problem after SEC Consult contacted the relevant authorities on 4 July this year. It updated the software and released it for general download on Wednesday 28 October.mExploiting the vulnerability would have required an attacker to have control of the eIDAS node or impersonate one, and the researchers point out that another study of eIDAS security last year didn't pick up the bug. That makes it highly possible that it was only recently introduced, they concluded.

Read More at NakedSecurity

More #News

- Ubisoft reports 93% drop in DDoS attacks after pushing back against attackers

- Facebook launches $2m suit against alleged phishing, hacking sites
- Takeaways from the $566M BriansClub breach
- New Office 365 Phishing Scams Using Audio Voicemail Recordings
- Chinese Hackers Compromise Telecom Servers to Spy on SMS Messages
- Leading Web Domain Name Registrars Disclose Data Breach
- 5 Places Where Hackers Are Stealthily Stealing Your Data In 2019
- Skimming Malware Found on American Cancer Society Webstore
- Bed Bath & Beyond Discloses Customer Login Credentials Breach
- Australia Cyber Threat Landscape report (H1 2019)
- Office 365 Enables ARC for Enhanced Anti-Spoofing Detection
- Adobe left 7.5 million Creative Cloud user records exposed online
- UniCredit reveals data breach exposing 3 million customer records
- Pwn2Own Hacking Event Expands to Industrial Control Systems
- Sixth June Fashion Site Hacked to Steal Credit Cards
- Joker's Stash Lists 1.3 Million Stolen Indian Payment Cards
- Fast-Food Chain Krystal Investigates Card 'Security Incident'
- New 'unremovable' xHelper malware has infected 45,000 Android devices
- Microsoft: Russian hackers are targeting sporting organizations ahead of Tokyo Olympics
- Assessing your Zero Trust readiness with the Microsoft Maturity Model
- 20 Companies Pledge Support for the Hack_Right Program
- Marriott Reports Exposure of Associates' Social Security Numbers
- WhatsApp launches fingerprint security lock support for Android devices

#Patch Time!

- PHP team fixes nasty site-owning remote execution bug
- New Chrome 0-day Bug Under Active Attacks – Update Your Browser Now!

#Tech and #Tools

- VB2019 paper: Inside Magecart: the history behind the covert card-skimming assault on the e-commerce industry
- Ghidra 9.1 is out
- Announcing cfnts: Cloudflare's implementation of NTS in Rust
- Istio Security: Zero-Trust Networking
- Public keys are not enough for SSH security
- Covenant: Developing Custom C2 Communication Protocols
- DNS Encryption Explained
- Abusing HTTP hop-by-hop request headers
- OffensiveCloudDistribution: Terraform and AWS to distribute large security scans across numerous cloud instances.
- Race Condition in Web Applications
- Hookers.nl breach: cracking 57% of the passwords in three days
- Exploiting prototype pollution – RCE in Kibana (CVE-2019-7609)
- NFC Beaming Bypasses Security Controls in Android [CVE-2019-2114]
- Introducing Csper!: simple report-only CSP policy (HTTP Header) on your website

- Introducing Cspell:: simple report-only CSP policy (HTTP Header) on your website.
- Arjun: HTTP parameter discovery suite.
- concerto: create TLS certificates for development purposes (C#).
- Practical Approaches for Testing and Breaking JWT Authentication
- SOCless: SOCless is a serverless framework built to automate incident response and operations processes.
- sadcloud: standing up (and tearing down!) purposefully insecure cloud infrastructure
- Abusing the SYLK file format
- Bypassing Authentication on SSH Bastion Hosts
- Persistence – Port Monitors
- The Path to CISO

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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