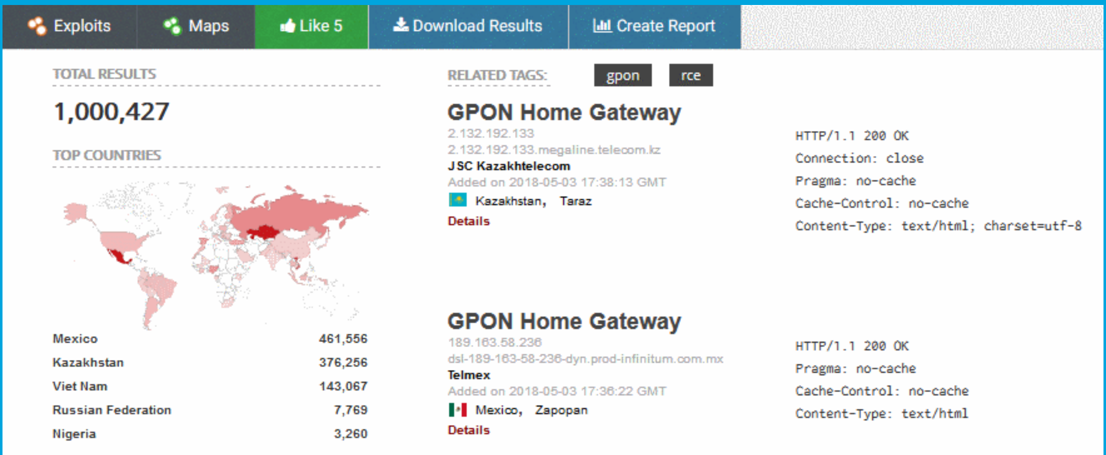
kindred

Security Newsletter

14 May 2018

Subscribe to this newsletter

Vulnerabilities Affecting Over One Million Dasan GPON Routers Are Now Under Attack



TOTAL RESULTS

1,000,427

TOP COUNTRIES

Mexico	461,556
Kazakhstan	376,256
Viet Nam	143,067
Russian Federation	7,769
Nigeria	3,260

RELATED TAGS: gpon rce

GPON Home Gateway
2.132.192.133
2.132.192.133.megaline.telecom.kz
JSC Kazakhtelecom
Added on 2018-05-03 17:38:13 GMT
Kazakhstan, Taraz
Details

```
HTTP/1.1 200 OK
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
```

GPON Home Gateway
189.163.58.236
dsl-189-163-58-236-dyn.prod-infinitum.com.mx
Telmex
Added on 2018-05-03 17:36:22 GMT
Mexico, Zapopan
Details

```
HTTP/1.1 200 OK
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```

Two vulnerabilities affecting over one million routers, and disclosed earlier this week, are now under attack by botnet herders, who are trying to gather the vulnerable devices under their control. Exploitation of these two flaws started after on Monday, April 30, an anonymous researcher published details of the two vulnerabilities via the VPNMentor blog.

His findings detail two flaws —an authentication bypass (CVE-2018-10561) and a remote code execution vulnerability (CVE-2018-10562). The most ludicrous of these two flaws is the first, which basically allows anyone to access the router's internal settings by appending the "?images" string to any URL, effectively giving anyone control over the router's configuration. By combining these two issues, the anonymous researcher said he was able to bypass authentication and execute code on vulnerable devices. A video by the VPNMentor crew summarizes the findings.

Within just 10 days of the disclosure of two critical vulnerabilities in GPON router at least 5 botnet families have been found exploiting the flaws to build an army of million devices. Security researchers from Chinese-based cybersecurity firm Qihoo 360 Netlab have spotted 5 botnet families, including Mettle, Muhstik, Mirai, Hajime, and Satori, making use of the GPON exploit in the wild.

Even if there is no official patch available, users can protect their devices by disabling remote administration and using a firewall to prevent outside access from the public Internet. Making these changes to your vulnerable router would restrict access to the local network only, within the range of your Wi-Fi network, effectively reducing the attack surface by eliminating remote attackers.

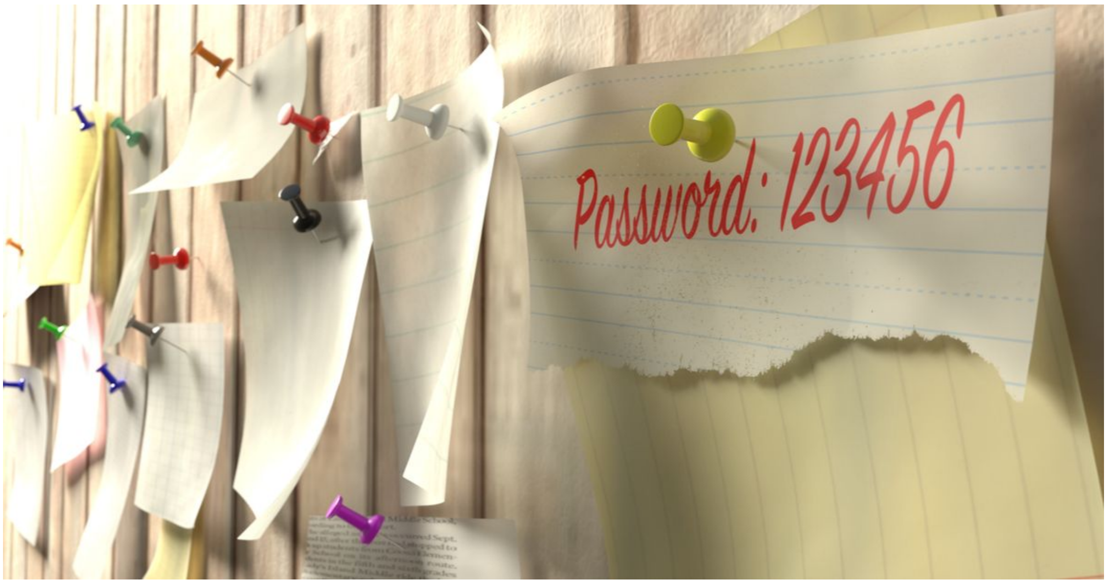
If you are unsure about these settings, vpnMentor has done this job for you by providing an online "user-friendly" solution that automatically modifies your router settings on your behalf, keeping you away from remote attacks.

Read More

5 Powerful Botnets Found Exploiting

Tool to Protect Dasan GPON Routers from Remote Hacking

Password re-use is dangerous, what about stopping it with password-sharing?



Two professors believe they have a way to stop password reuse, which is giving hackers access to more and more information every day. Their plan involves 20-50 of the biggest websites on the internet coordinating and forcing users to create different passwords for all of their sites.

The traditional solution is to implore users to set unique ones, preferably using a password manager. However, only a small minority pay any attention. But what if there were a way for websites to compare notes on whether a password (or similar password) has been set by a user elsewhere?

At the outline level it's easy: a server where the user is registering a new account – the requester – asks other sites (responders) whether that individual has used the same password with them. However, that has to be done in a way that protects those passwords (the sites can only say "yes" or "no", without handing around a password); the sites also have to identify the right user; and the scheme would have to avoid imposing excessive overheads on authentication servers.

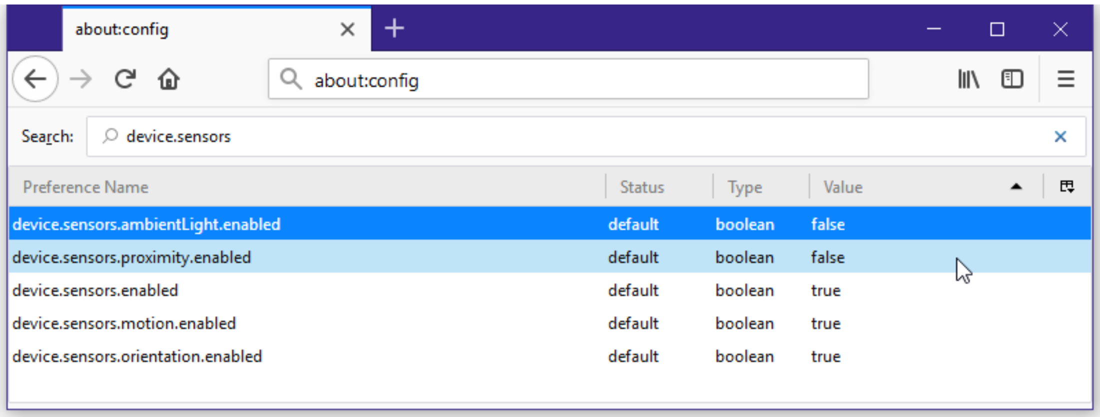
Their suggestion is the 'private set-membership-test' protocol, based on the seeming magic of homomorphic encryption invented by IBM a decade ago to process encrypted cloud data without needing to decrypt it first.

For identification, they reckon (probably correctly) that the vast majority of users rely on email addresses tied to a single domain from within this select group. As for security and privacy (the problem of querying sites without creating the potential for leakage), the principles of homomorphic encryption would take care of this, they say.

Read More

Even More

Firefox 60 Supports Enterprise-Friendly Policy Engine and Password-free login capabilities



about:config

Search: device.sensors

Preference Name	Status	Type	Value
device.sensors.ambientLight.enabled	default	boolean	false
device.sensors.proximity.enabled	default	boolean	false
device.sensors.enabled	default	boolean	true
device.sensors.motion.enabled	default	boolean	true
device.sensors.orientation.enabled	default	boolean	true

The Mozilla Foundation released Firefox 60 earlier today. The highlights of this new Firefox version are support for a policy engine for deploying Firefox across enterprise environments, support for the WebAuthn passwordless authentication system, and the addition of sponsored stories (ads) for US users.

By far the biggest addition to Firefox 60 is the new Group Policy engine that allows system administrators in large corporate networks to deploy and control Firefox settings across an entire company via group policy objects. Other browsers like Chrome, Edge, and IE had a similar feature for years, and this was one of the most requested features in Firefox for a long time.

An emerging W3C standard called Web Authentication or WebAuthn, is enabled by default in Firefox 60 and is coming later this month to Chrome 67, and Microsoft Edge. It's also under consideration for Safari. By removing passwords, the WebAuthn API will make phishing attacks a lot harder and gives users more convenient authentication choices, including hardware security key dongles such as a YubiKey device, fingerprint readers on smartphones, or facial-recognition systems like the iPhone X's Face ID.

Firefox 60 also comes with support for same-site cookies, a mechanism that prevents malicious websites from requesting other sites' cookies. Mozilla engineers added support for this feature to improve both user privacy, but also as a way to prevent some types of cross-site request forgery (CSRF) attacks that relied on malicious sites faking actions on other sites by employing cookies they shouldn't have had access to.

Read More

Even More

Backdoored libraries are getting common, be careful what you use

The Node Package Manager (npm) team avoided a disaster recently when it discovered and blocked the distribution of a cleverly hidden backdoor mechanism inside a popular —albeit deprecated— JavaScript package. The actual backdoor mechanism was found in "getcookies," a relatively newly created npm package (JavaScript library) for working with browser cookies. The npm team —who analyzed this package earlier today after reports from the npm community— says "getcookies" contains a complex system for receiving commands from a remote attacker, who could target any JavaScript app that had incorporated this library. Back in August 2017, the same npm team removed 38 JavaScript npm packages that were caught stealing environment variables from infected projects.

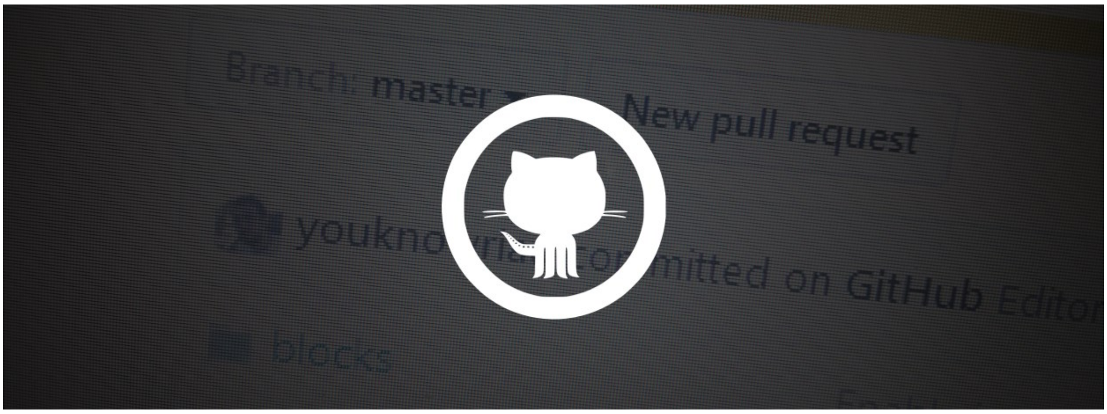
Something similar happened on PyPI — Python Package Index — the official third-party software repository for the Python programming language. Back in September 2017, the Slovak National Security Office (NBU) found and reported ten malicious Python packages on PyPI, which were promptly removed.

Barely a week has passed from the last attempt to hide a backdoor in a code library, and we have a new case. This time around, the backdoor was found in a Python module. The module's name is SSH Decorator (ssh-decorate), developed by Israeli developer Uri Goren, a library for handling SSH connections from Python code. On Monday, another developer noticed that multiple recent versions of the SSH Decorate module contained code that collected users' SSH credentials and sent the data to a remote server. After having the issue brought to his attention, Goren said the backdoor was not intentional and was the result of a hack.

Somebody Tried to Hide a Backdoor in a Popular JavaScript npm Package

Backdoored Python Library Caught Stealing SSH Credentials

Github and Twitter accidentally recorded some plaintext passwords in their logs



In an email sent out last week, GitHub has warned a select number of users that a bug in its password reset functionality has recorded users' passwords in plaintext format inside the company's internal logs. The company says that the plaintext passwords have only been exposed to a small number of GitHub employees with access to those logs. No other GitHub users have seen users' plaintext passwords. GitHub says that normally, passwords are secure, as they are hashed with the bcrypt algorithm. The company blamed a bug for plaintext passwords ending up in its internal logs. Only users who've recently reset passwords were affected. GitHub said it discovered its error during a routine audit and made it clear its servers weren't hacked.

In June 2016, GitHub also sent out password reset emails to customers after an unknown actor tried to access GitHub accounts using passwords leaked online at the time, via the LinkedIn, Dropbox, MySpace, and the other mega breaches of 2016.

Twitter just asked all 300+ million users to reset their passwords, citing the exposure of user passwords via a bug that stored passwords in plain text — without protecting them with any sort of encryption technology that would mask a Twitter user's true password. The social media giant says it has fixed the bug and that so far its investigation hasn't turned up any signs of a breach or that anyone misused the information. But if you have a Twitter account, please change your account password now.

Agrawal explains that Twitter normally masks user passwords through a state-of-the-art encryption technology called "bcrypt," which replaces the user's password with a random set of numbers and letters that are stored in Twitter's system. Due to a bug, passwords were written to an internal log before completing the hashing process," he continued. "We found this error ourselves, removed the passwords, and are implementing plans to prevent this bug from happening again

Read More

Twitter admits to password storage blunder

Cutting room floor

- Windows CLI Apps Vulnerable to New Ctrl-Inject Process Injection Attack
- What is a Chief Security Officer? Understanding this critical role
- Critical bug in 7-Zip – make sure you're up to date!
- Microsoft Patch Tuesday, May 2018 Edition
- Security pros: Get ready to patch for 8 new Spectre-related vulnerabilities soon
- Abbott to fix critical vulnerabilities in 350,000 ICDs & Pacemakers
- GLitch: New 'Rowhammer' Attack Can Remotely Hijack Android Phones
- New Service Blocks EU Users So Companies Can Save Thousands on GDPR Compliance
- Amazon Introduces AWS Security Specialty Certification Exam
- Facebook's Phishing Detection Tool Now Recognizes Homograph Attacks
- Phishing alert: GDPR-themed scam wants you to hand over passwords, credit card details
- Microsoft Issues Emergency Patch For Critical Flaw In Windows Containers
- Australian Bank Lost Data for 19.8 Million Accounts
- Amazon Follows Google in Banning "Domain Fronting"

#Tech and #Tools

- Download Kali Linux 2018.2 with new security features
- SANS Poster - Windows Forensic Analysis
- Python Exploit for Remote Code Execution on GPON home routers (CVE-2018-10562)
- Javascript CoinHive in Excel
- RouterSploit 3.0: Exploitation framework for embedded devices
- ShellPop: Pop shells like a master.
- Domain Fronting and Host header obfuscation
- Passphrase wordlist and hashcat rules for offline cracking of long, complex passwords
- Project Sonar: An Underrated Source of Internet-wide Data

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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