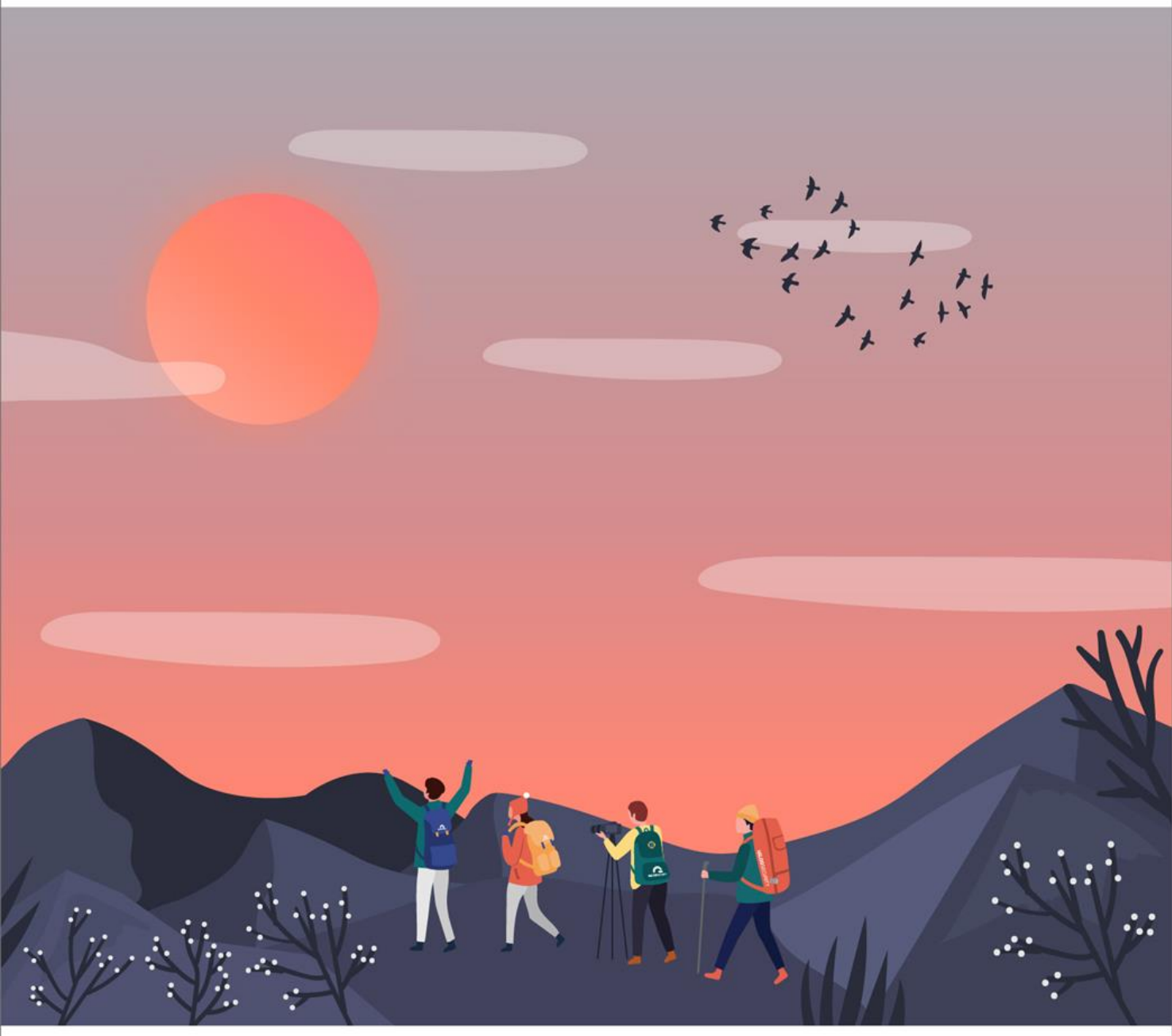
Monthly Security Report

2020
January



Cover Story

How to use command Log and its hardening
Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

IGLOOSECURITY

This report is based on the data collected through the SIEM solution at IGLOO SECURITY's Security Operation Center (SOC). IGLOO SECURITY continuously strives to achieve a 24/7 safe cyber environment throughout the year.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

- Monthly attack service and trend analysis
- Detailed analysis according to different patterns

3. SIEM Guide (SPiDER TM V5.x)

- How to use command Log and its hardening

4. Tech Note

- Oracle WebLogic RCE vulnerability
  (CVE-2019-2890) analysis and response

5. Focus On IGLOO Security

- This month's IGLOO Security

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 1

Monthly Security Issue

1. Security issue

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Security Issue

New Orleans City of USA administration system was paralyzed … $ 1.1 billion in damage from a single phishing email clicked by a city employee

- The city of New Orleans was attacked by cyber attacks, with more than 450 servers and 3,500 endpoint devices infected by ransomware.
- New Orleans City declared a state of emergency paralyzed on 13 December. In addition, The city explain that a city official clicks on a phishing email and it became an attack start.
- The attacker used a variant of the Ryuk ransomware and There was no request for a decryption fee from the attacker, and no information was leaked.
- The city of New Orleans has opened the War Room, an exhibition operation room. The plan is to oversee the recovery process through Warroom so that there is no additional impact on the Dashmin service.
- The financial damage to New Orleans was estimated to be more than $ 1 million.

Emerging Vietnamese hacking group attempts to infiltrate global automobile manufacturer's network to seize IPR

- Hacking organizations suspected of being associated with the Vietnamese government have entered the global automobile manufacturer's network, attempting to seize IP rights.
- On December 23, Bloomberg News reported that a Vietnamese hacking organization known as APT32 has been targeting the global automotive industry for the past two years.
- According to security company CrowdStrike, APT32 has attempted to penetrate the network by opening a domain that pretends Toyota and Hyundai.
- Vietnam is ranked next to Russia and China to rapidly increase their cyber capabilities. Vietnamese hacking organizations have evolved by imitating the techniques of Chinese hacking organizations and are attacking not only intellectual property rights but also foreign government agencies, journalists and dissidents related to Vietnamese politics.

Warning for malicious mail disguised as security mail from banks

- Emails disguised as security emails from specific banks are distributed and require special attention from users.
- The message contains an html attachment, which when clicked, prompts you for a six-digit date of birth, just like a regular email security email.
- The attacker tries to download an Excel document by entering a password, which contains a malicious macro that can send system information to C&C, including the computer name, user name, OS information, and the name of the currently running process.
- Security experts are requesting for special attention that the malicious mail is currently being distributed in large quantities.

US Alaska Airlines Cancels All Flight Departures due to Cyber Attacks

- Aircraft RavenAir, headquartered in Anchorage, Alaska, was attacked by a cyber attack, resulting in a total cancelling all flights on the morning of December 21. Six flights were canceled, leaving more than 260 passengers uncomfortable.
- Attackers have turned out to be targeting the "De Havilland Canada" Dash-8 aircraft, which is often used by smaller airlines. The carrier, which catches signs of attack, blocks the connection between the dash-8 maintenance system and the backup system to prevent accidents.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Security Issue

More cyber attackers use cloud servers as command control (C2) servers

- According to the security industry, attacks that the number of spread malware using cloud servers as command control (C2) servers is increasing. C2 is a server that sends spam mails to PCs already infected with malware and commands DDoS attacks. It is mainly operated by hackers.
- In the past, C2 of a specific target company was mainly used for attack, but recently, it has been changed by putting malware communication infrastructure in cloud server, continuously communicating with it, and launching cyber attacks.
- For example, if a user's PC is already infected, hackers can send additional malicious files through the cloud.
- Security experts predict that these attacks will increase as the number of users of cloud-based services increases.

Personal information leaked to 260 million Facebook users

- According to a report on Dec. 22, 260 million personal information of Facebook users were leaked.
- According to a report by security consultant Bob Diachenko from Ukrainian and security firm ‘Comparytech, personal information such as IDs, names and phone numbers of 268 million Facebook users were ‘disclosed on the Internet. 99% of leaked information was American users and rest of them were Vietnamese.
- Diachenko said that the personal information database was open for at least ten days from December 4, and five days had passed since he informed the ISP managing the server's IP address.
- Facebook is investigating the situation, assuming that the Vietnamese hacker group is involved.

Malicious Insiders Sell Information and Earn pocket money on Dark Web

- According to security experts who conduct dark web research, more companies and organizations are selling information from their group on the dark web at lower prices to get personal income.
- According to security firm IntSights, insiders were mostly captured on the Russian Dark Web and sell information on it.
- Surveys show that brokers are subscribing to insiders after verifying the insiders' access rights and capabilities. Once passed, the insider was protected from disclosure.
- Security experts believe that this will be a major problem in that it will enable targeted attacks against key people such as VIPs and financial institutions.

TikTok, leak personal information and collect user location information?

- TikTok, serviced by Chinese startup Bite Dance, is an SNS that communicates based on a 15-second short video. The average monthly usage is 1.5 billion people worldwide.
- According to TikTok's Terms of Service, SIM cards and IP addresses containing personal information may be leaked automatically without the consent of the legal representative.
- In addition, suspicion that TikTok is a spy app of the Chinese government has been raised all over the world. TikTok states that if we allow access, we collect satellite location system (GPS) information and mobile device location information.
- Security experts say it is not easy to apply sanctions solely in context because of trade frictions and other issues.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 2

IGLOO Statistics

1. Monthly attack service and trend analysis
   - 01. Top 10 monthly attack service(port)
   - 02. Monthly attack service(port) cases compared to previous month
   - 03. Top 10 monthly attack service patterns
   - 04. Monthly attack service incident patterns compared to previous month
2. Detailed analysis according to different patterns

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted

01. TOP 10 monthly attack service(port)

Event analysis collected over a month in January 2020 shows that events using Oracle (TCP/1521) ports have been on an upward trend. In addition, event history using DNS (TCP/443) and MS-SQL-S (TCP/1433) fell from the previous month. The total number of events has increased and this is confirmed by the effect of the increase in the number of HTTP (TCP/80) ports.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,731,022,144	53.23%	-
2	DNS(UDP/53)	557,349,635	17.14%	-
3	Microsoft-DS(TCP/445)	387,710,916	11.92%	-
4	HTTPS(TCP/443)	249,346,957	7.67%	-
5	ICMP(0/ICMP)	114,461,010	3.52%	-
6	SNMP(UDP/161)	96,726,105	2.97%	-
7	Telnet(TCP/23)	38,886,138	1.20%	-
8	Orcale(TCP/1521)	27,334,576	0.84%	▲2
9	DNS(TCP/53)	25,046,221	0.77%	▼1
10	MS-SQL-S(TCP/1433)	24,152,655	0.74%	▼1
	Total	3,252,036,357	100.00%	-

[Table2-1] TOP10 monthly attack patterns

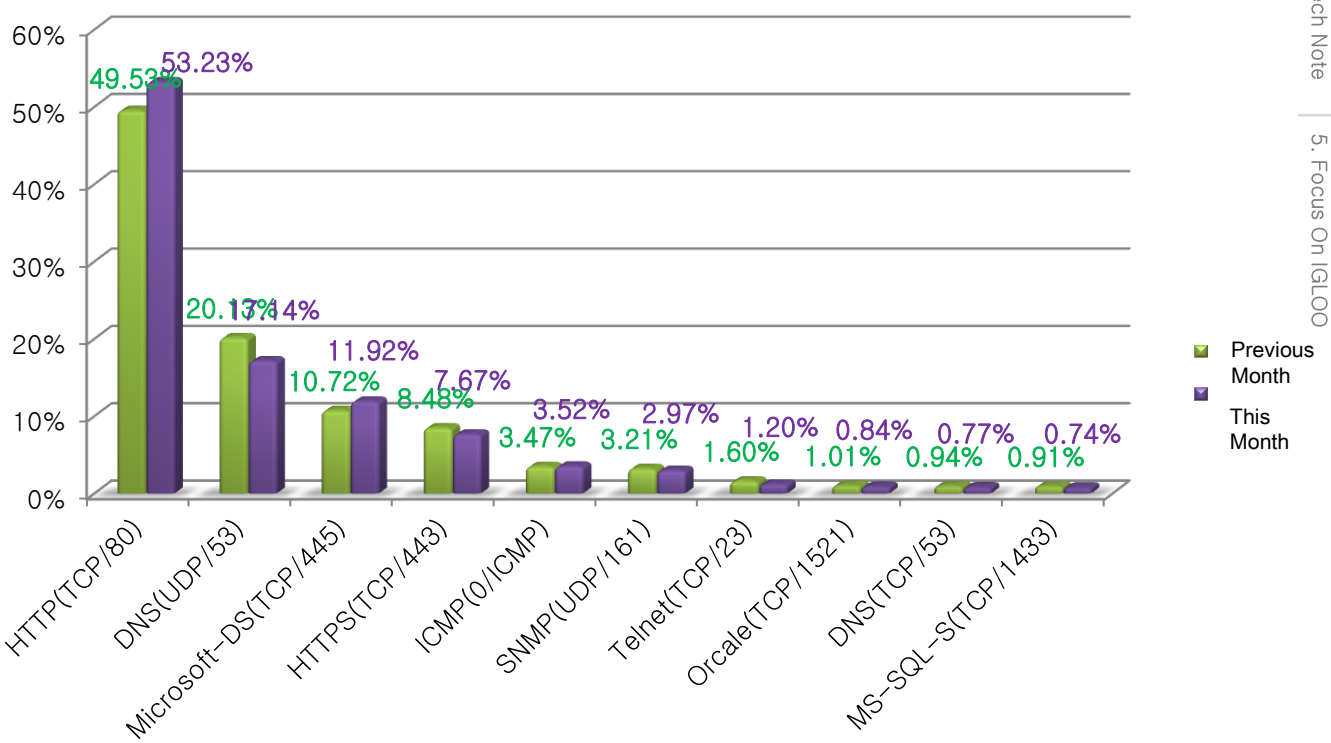
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted

02. Monthly attack service(port) cases compared to previous month

As a result of event analysis by attack service port, the rate of change was lower within 2% compared to the previous month, and the number of accesses of HTTP (TCP/80) and Microsoft-DS (TCP/445) service ports increased. The HTTP service is judged to be caused by the increase in flooding events for the web server, and it is necessary to control abnormal overaccess of a single user through threshold blocking. It is recommanded to use firewall policy setting so that only authorized users can access the TCP/445 port.



[Figure 2-1] TOP10 monthly attack port

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The trend of attack patterns detected by IGLOO SECURITY SOC can be used to identify the trend of the latest attacks.

03. TOP 10 monthly attack service patterns

In January 2020, the ranking of the HTTP POST Session Exhaustion Attack (By rudy) event decreased significantly, and the ranking of the Multi Packet Inspection event increased in the TOP10 attack pattern. The ranking of many other events seems to have increased, but this may be due to the fall in the ranking of HTTP POST Session Exhaustion Attack (By rudy) events.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	975,262,288	94.91%	-
2	ACK Port Scan(F/W Scan)	11,589,878	1.13%	▲1
3	HTTP Connection Limit Exhaustion Attack(By Slowloris)	11,509,480	1.12%	▲1
4	Multi Packet Inspection	11,325,548	1.10%	▲3
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	5,895,348	0.57%	-
6	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	3,735,350	0.36%	▲2
7	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	3,465,950	0.34%	▼1
8	HTTP Login Brute Force	2,643,834	0.26%	▲1
9	HTTP POST Session Exhaustion Attack(By rudy)	1,513,704	0.15%	▼7
10	HEAD / HTTP (Http server buffer overflow)	590,764	0.06%	NEW
Total		1,027,532,144	100.00%	-

[Table 2-2] TOP10 monthly attack pattern

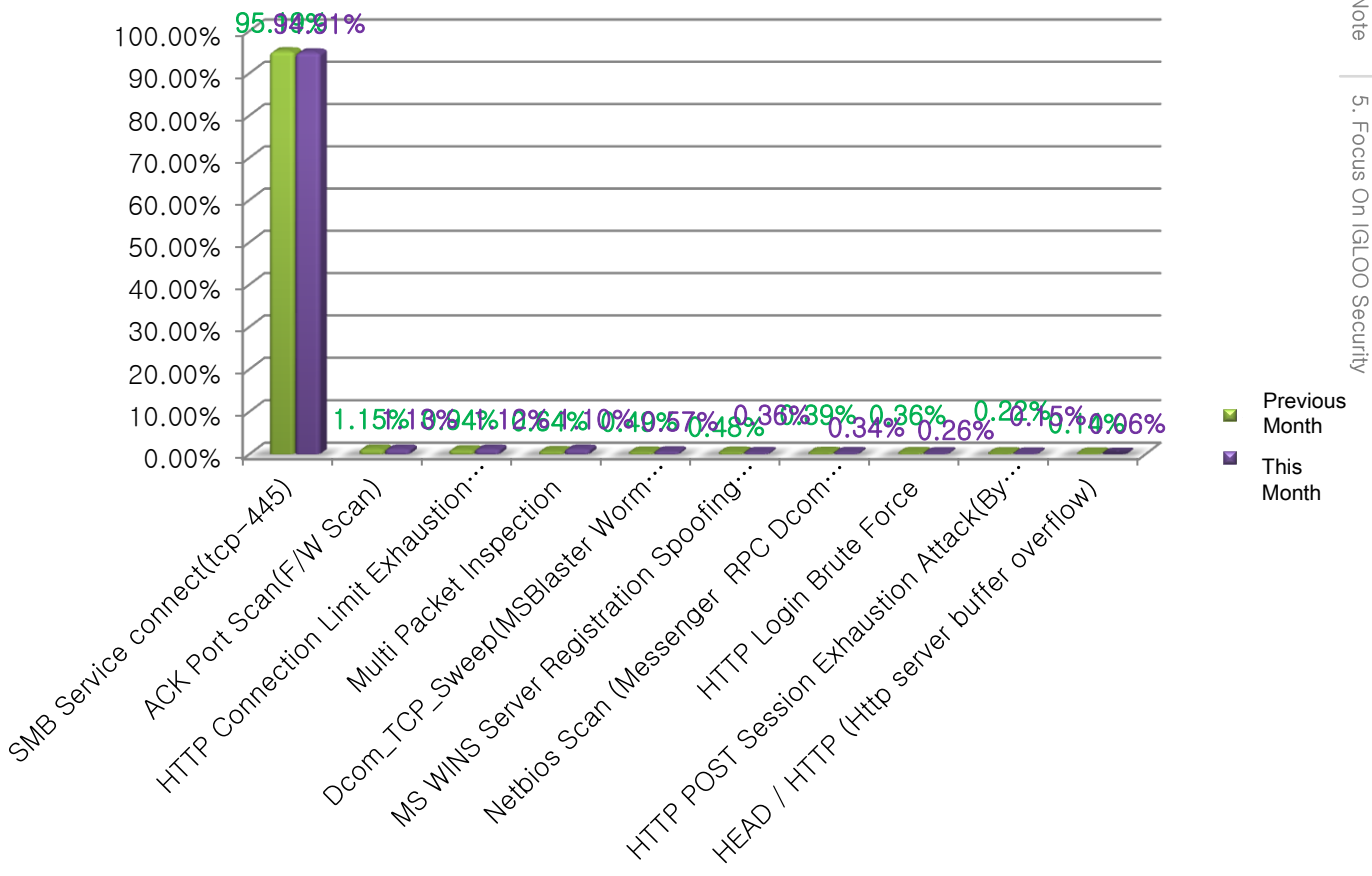
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The attack pattern rankings detected by IGLOO SECURITY SOC can be used to identify the latest trends of attacks.

04. Monthly attack service incident patterns compared to previous month

Multi Packet Inspection events increased compared to the previous month. This event is an IPS rule that detects packet repetition of the same pattern with a packet size of more than Bytes. It is necessary to prepare for these denial of service attacks by calculating appropriate pps for each service. In addition, HEAD/HTTP (Http server buffer overflow) is newly ranked. The HEAD method is similar to the GET method, but the method is used to quickly receive only header information from the web server. It is recommanded to take measures so that unnecessary information is not exposed due to the security device blocking policy for unused methods.



[Figure 2-2] TOP10 monthly attack pattern

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

2 Detailed analysis according to different patterns

The detailed analysis results according to the attack pattern occurred in January are introduced. It is necessary to take precautionary measures against the vulnerability of the relevant system by referring to the detailed analysis result for each detection pattern.

Attack Pattern	Detailed Analysis Results
SMB Service connect(tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
ACK Port Scan (F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP request to a web server, unlike a DoS attack that transmits a large amount of packets. The target web server may be depleted of connection resources. After the connection resources are depleted, the target web server may be in a denial of service state that cannot respond to user requests.
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS.It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
Dcom_TCP _Sweep (MSBlaster Worm Messenger)	W32.Blaster.Worm is a worm that spreads by using the DCOM RPC Buffer Overflow vulnerability. The worm checks whether the TCP / 135 port is enabled and infects the system when it is found. The infected system activates TCP / 4444 port, downloads malicious files from the host server, registers them in the registry, and in this process, traffic from the infected system may increase.
MS WINS Server Registration Spoofing Vuln-1[Req] (UDP-137)	NetBios checks each other's information through UDP port 137, establishes session with TCP 139, and exchanges data through TCP 138. An attacker can use this UDP port 137 to establish a session with the target system and scan information about the folders and networks shared with the target system.
Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	A network scanner tool that scans all computers in the IP addresses range you choose, using NetBIOS protocol. For every computer located by this NetBIOS scanner, the following information is displayed: IP Address, Computer Name, Workgroup or Domain, MAC Address, and the company that manufactured the network adapter (determined according to the MAC address). NetBScanner also shows whether a computer is a Master Browser. You can easily select one or more computers found by NetBScanner, and then export the list into csv/tab-delimited/xml/html file.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
HTTP POST Session Exhaustion Attack(By rudy)	R.U.D.Y stands for "R-U-Dead-Yet" and is a connection resource depletion type Denial of Service tool using HTTP's POST method. Incomplete HTTP headers and fragmented data are used to generate a large number of non-terminating connections, exhausting the connection resources of the target system.
HEAD / HTTP (Http server buffer overflow)	HEAD requests, similar to HTTP GET requests, are commonly used when using scanners or collecting information by malicious users.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

- How to use Command Log and its hardening

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

SPiDER TM V5.0 is an integrated security management solution that combines security monitoring experience of Igloo Security and big data utilization to increase the agility and efficiency of monitoring business through unified monitoring environment from initial detection to log/network packet analysis.

Technical Support Center
Analysis Technique Team

01. Overview

When building and utilizing SIEM, the user's command history is considered to be collected. Since the Linux server does not take action until you enter a command, you can say that you can analyze the log only by properly collecting the access log and command log. In this article, learn how to harden the command log.

Log Type	Linux	AIX	HPUX	Solaris
Messages	○	○	○	○
wtmp/utmp	○	○	○	○
wtmpx/utmpx				○
Btmp	○		○	
Pacct	○	○	○	○
Lastlog	○	○	○	○
Sulog		○	○	○
Errlog		○		
Xfertog(FTP log)	○	○	○	○
audit.log	○			
Secure	○			
Syslog		○	○	○
History	○	○	○	○
authlog				○

[Table 3-1] Linux/Unix Log

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

02. How to harden History log

By default, commands entered by the user are saved in the ~$HOME/.bash_history file. However, if you collect the ~$HOME/.bash_history file in SIEM using a module that reads the history log file, it is difficult to use for correlation analysis and time series analysis as shown in [Figure 3-1].

Log	Sublog	Event Time	Origin IP	Origin Name	Product	Message
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	cd work/
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	cd 2019-09-24
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	ls
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	cd ..
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	cd ..
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	ls
system	history	2020/01/06 16:37:30	192.168.1.100	SIEM_MANAGER	linux	cd ..

RAW = historycd .. , attack = - , category = null , count = 1 , d_info = - , d_ip = - , d_port = - , event_time = 20200106163730512 , id = 20200106163730512_0000000000563771402_20200106.log_LINUX-HISTORY-2441 , log = system , logtype = SYS , method = - , mgr_ip = 192.168.1.100 , mgr_time = 20200106163730512 , msg = cd .. , origin = 192.168.1.100 , origin_id = 2441 , origin_name = SIEM_MANAGER , product = linux , protocol = 6 , risk = 3 , s_info = - , s_ip = - , s_port = - , status = 999 , sublog = history , work_time = 16

[Figure 3-1] history log

The history log has a feature that is saved in the ~$HOME/.bash_history file when the terminal closed. Due to this feature, the terminal closing time is collectively collected in the SIEM as shown in [Figure 3-1]. In addition, the connected IP, the user, the directory where the command is executed, and whether or not the command is successful are not left.

Let's think from the attacker's point of view. Attackers can use a command such as kill-9 $$ to force the shell itself to abort and not save the command log after logging in, so that it is not saved in the history log file. Alternatively, you can delete it with the history-c option. In addition, you can use the ln –s/dev/null .bash_history command to link .bash_history to /dev/null or even create a ~$HOME/.bash_history directory to prevent files from being created. So let's just set it up to make up for the shortcomings of this history log.

1) How to configuration

Add configuration at the bottom of / etc / profile as shown in [Figure 3-2].

```
remoteip=$(who -m | awk -F₩( '{print $2}' | sed "s/[()]//g" )
if [[ -z $remoteip ]]; then remoteip=localhost; fi
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p local6.debug "$(whoami) $remoteip
[$$] [$RETRN_VAL] [$PWD]: $(history 1 | sed "s/^[ ]*[0-9]₩+[ ]*//" )"'
readonly PROMPT_COMMAND
```

[Figure 3-2] /etc/profile Configuration

With PROMPT_COMMAND, the contents inside the PROMPT_COMMAND variable are executed just before the prompt. In other words, the user's command log can be saved as a file in a desired form in real time.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

The addition of readonly here is to make it impossible for the user to override or unset PROMPT_COMMAND arbitrarily.

Next, add the configuration as shown in [Figure 3-3] at the bottom of the syslog configuration file and restart the syslog daemon.

```
local6.*                /var/log/(name of logfile).log
```

[Figure 3-3] SYSLOG configuration

The command log as shown in [Figure 3-4] can be saved in real time. The log format is as follows:
* Name of Time Host Access Account: IP of Command Execution Account Access [Shell PID]
[Execute Result (0: Failure other than 0) [Command Execution Path]: Execution Command

```
Jan  5 18:42:50 web3 root: root 118.221.222.15 [1176] [0] [/var/log]: whoami
Jan  5 18:42:54 web3 root: root 118.221.222.15 [1176] [0] [/var/log]: cat /etc/passwd
```

[Figure 3-4] command log format

03. Utilizing the Command Log in SIEM

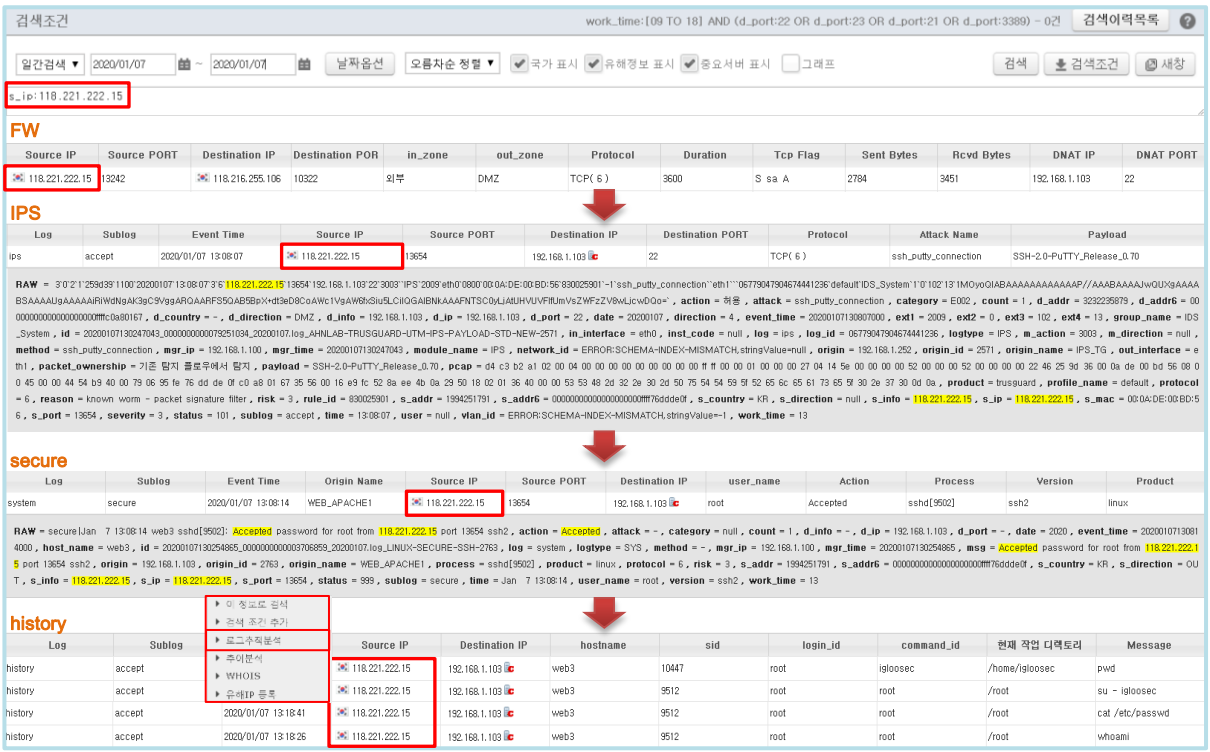
As mentioned above, many of the shortcomings of history logs can be solved by configuring the command log hardening.

1. Command logs can be collected and utilized in SIEM in real time.
2. Command logs of all accounts can be collected and utilized in real time.
3. The su (substitute user) can be known by the access account and the command execution account.
4. You can see whether the command succeeded.
5. You can see whether history log is deleted.
6. Correlation analysis can be performed via access IP.

By hardening the command log, you can hunt down the attacker's behavior from the perimeter security device (FW, IPS) to the endpoint server (shown as [Figure 4-5]) by searching for (s_ip: attack IP). You can check the /etc/password file and su to the igloosec account after accessing the server SSH port 192.168.1.103 through Putty through root in the internal DMZ from the outside of the first firewall.

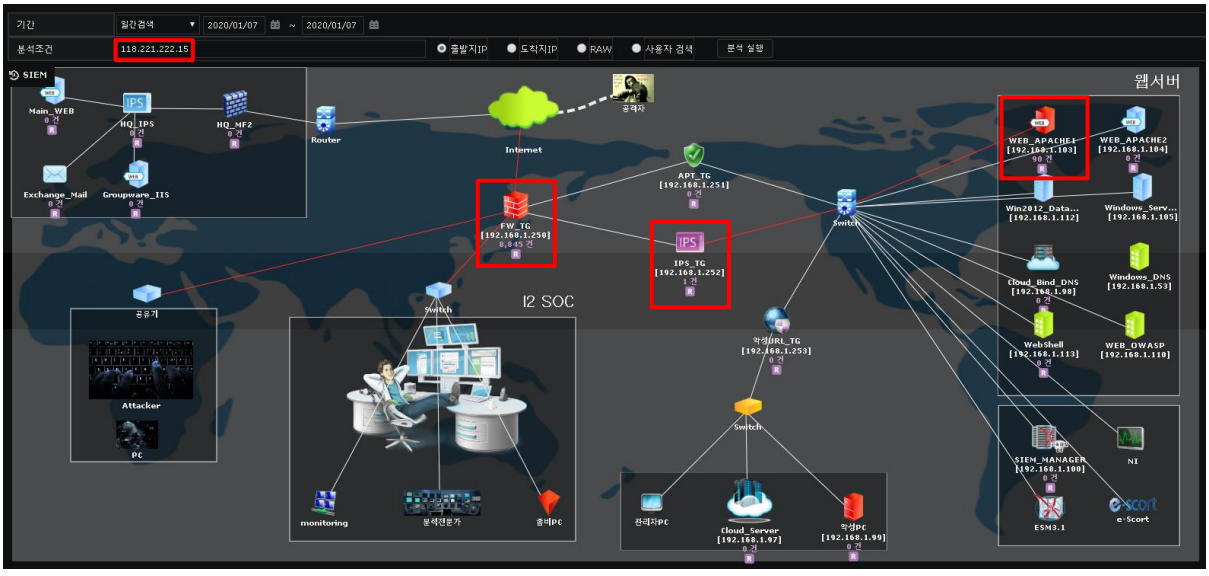
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening



[Figure 3-5] Attacker Log Search

Log trace analysis on the results hunted through the log search provides a more visual view of the attack path, targets, and attack flow to the endpoint.



[Figure 3-6] Attacker log trace and analysis

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

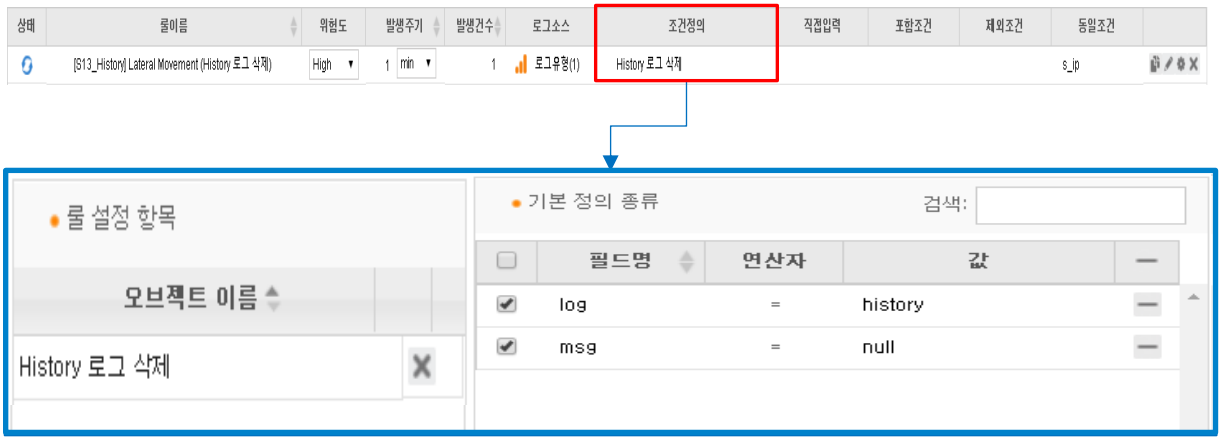
04. Using Command Log Alerts in SIEM

Command logs collected in SIEM allow us to alert in various scenarios. There are abnormal behavior alerts that generate an alert when a command log occurs on weekends, holidays, and nightly after work, detection alerts for command log access IPs in connection with CTI, and audit alerts for specific command execution such as mounts on outsourced IPs.

Many security monitoring centers generate and analyze alerts focused on perimeter security equipment, but traditional perimeter security equipment centers (FW, IPS, WAF) make it difficult to capture an attacker's Lateral Movement. The alert I'm going to introduce is about the attacker's Lateral Movement. If the attacker's clearing of the history log was a special behavior in the past, most recent attackers delete the history log after the attack. Since the attacker's actions every time the internal movement of the host attack is the history log deletion, monitoring only the history log deletion can be identified before the attacker achieves the final goal in the target attack.

1) Internal network movement (History log deletion) Single rule detailed setting

The command log collected via command hardening will be null if no ~$HOME/.bash_history log has been cleared. With this log feature, you can set a single alarm rule as shown in [Figure 3-7].



[Figure 3-7] Single alert rule configuration

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

2) Detection result

If the attacker cleared the history log with a single command such as kill -9 $$, history -c, etc., one-time alert would be generated as shown in [Figure 3-8]. If the attacker cleared the history log with a single command such as kill -9 $$, history -c, etc., one-time alert would be generated as shown in [Figure 3-8]. However, if you linked the .bash_history to /dev/null using the ln –s/dev/null.bash_history command or created the ~$HOME/.bash_history directory to prevent the file from being created, the alert will be triggered whenever the user logs in.

[Figure 3-8] Detailed Analysis of Detection Results

05. Command Log hardening with Snoopy Logger

Although I explained how to harden the command log, there are limitations to that approach. Changing to csh or another shell, ssh account @ IP (command) remote command execution, reverse shell, commands via webshell, etc. There is a tool for logging all commands from scripts on these servers. Snoopy Logger is the tool. It can be downloaded from https://github.com/a2o/snoopy.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

1) How to configuration

Snoopy Logger must specify the log format in the /etc/snoopy.ini file. The log format can be used as shown in [Figure 3-9].

```
; - %{cmdline}       ; (available=yes) Full command line, with arguments
; - %{cwd}           ; (available=yes) Current working directory
; - %{datetime}      ; (available=yes) Date and time in ISO 8601 format
; - %{domain}        ; (available=yes) Domain of current system
; - %{egid}          ; (available=yes) Effective gid that executed the command
; - %{egroup}        ; (available=yes) Effective group name that executed the command
; - %{env:VAR}       ; (available=yes) Environmental variable named 'VAR'
; - %{env_all}       ; (available=yes) All environmental varibles, comma separated
; - %{euid}          ; (available=yes) Effective uid that executed the command
; - %{eusername}     ; (available=yes) Effective username that executed the command
; - %{filename}      ; (available=yes) Full path to executable
; - %{gid}           ; (available=yes) Group id that executed the command
; - %{group}         ; (available=yes) Group name that executed the command
; - %{hostname}      ; (available=yes) Hostname of current system
; - %{login}         ; (available=yes) Login name (tries getlogin_r() first, then SUDO_USER env variabe,
and LOGNAME env as last resort)
; - %{pid}           ; (available=yes) ID of process that executed the command
; - %{ppid}          ; (available=yes) Parent process ID of process that executed the command
; - %{rpname}        ; (available=yes) Root process name of process that executed the command
; - %{sid}           ; (available=yes) Process id of session group process leader
; - %{snoopy_threads} ; (available=yes) Number of threads that Snoopy currently is configured for
; - %{snoopy_version} ; (available=yes) Snoopy version
; - %{snoopy_literal:arg} ; (available=yes) Dummy data source, only returns its argument literally
; - %{tid}           ; (available=yes) Thread ID of process that executed the command
; - %{tid_kernel}    ; (available=yes) Thread ID of process that executed the command, as returned
by Linux kernel
; - %{timestamp}     ; (available=yes) Current Unix timestamp
; - %{timestamp_ms}  ; (available=yes) Millisecond part of current Unix timestamp
; - %{timestamp_us}  ; (available=yes) Microsecond part of current Unix timestamp
; - %{tty}           ; (available=yes) Which TTY the command was run on
; - %{tty_uid}       ; (available=yes) TTY uid
; - %{tty_username}  ; (available=yes) TTY username
; - %{uid}           ; (available=yes) User id that executed the command
; - %{username}      ; (available=yes) Username that executed the command
```

[Figure 3-9] Snoopy Logger Log Source

Refer to the [Figure 3-9] configuration or to write more detailed log, refer to [Figure 3-12] and modify the /etc/snoopy.ini file to enable snoopy logging through the snoopy-enable command.

```
message_format = "[login_id:%{login} command_id:%{username} rpname:%{rpname} uid:%{uid}
sid:%{sid} tty:%{tty} cwd:%{cwd} filename:%{filename}]: %{cmdline}“

output = file:/var/log/(name of log file).log
```

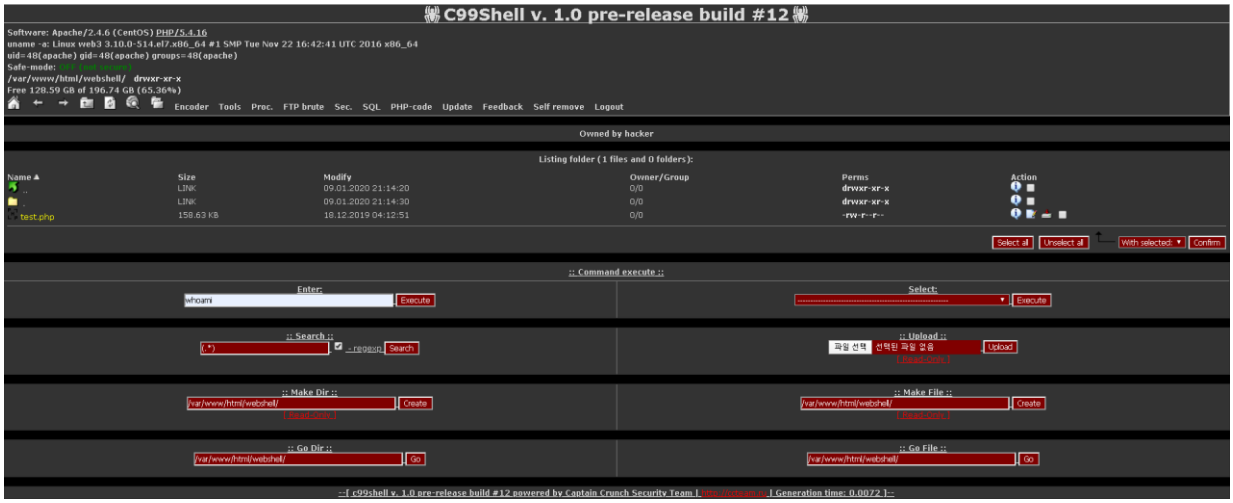
[Figure 3-10] Snoopy Logger log source

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

How to use command Log and its hardening

2) Webshell and Command Injection log

As shown in [Figure 3-11], when entering a command through the web shell, as shown in [Figure 3-12], the whoami command is executed in the /var/www/html/webshell directory with apache privileges instead of the normal login. In addition to the Webshell commands, all Command Injection logs are logged with apache privileges.



[Figure 3-11] C99Shell Webshell

Log	Sublog	Event Time	Origin Name	login_id	command_id	uid	tty	sid	rpname	현재 작업 디렉토리	Message
system	snoopy	2020/01/10 06:35:24	WEB_APACHE1	(unknown)	apache	48	(none)	9241	httpd	/var/www/html/webshell	id
system	snoopy	2020/01/10 06:35:24	WEB_APACHE1	(unknown)	apache	48	(none)	9241	httpd	/var/www/html/webshell	whoami

[Figure 3-12] Webshell command log

The attacker's signature in the web log is the POST to http_method. However, it is not easy to detect Webshell and command injection in POST log. However, if you use Snoopy Logger to store and utilize all command logs, you can detect Command Injection and Webshell more easily by taking advantage of the feature that Webshell or Command Injection executes commands with apache privileges.

06. Conclusion

As security strategies extend from outside defenses to proactive detection and response, much attention has been paid to identifying and responding to internal threats. Logs are the basis for finding and responding to threats in complex IT environments. Each log has a limit, but to overcome that limit, defenders must actively improve the log to detect and respond to threats.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 4

Tech Note

Oracle WebLogic RCE vulnerability (CVE-2019-2890) analysis and response

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

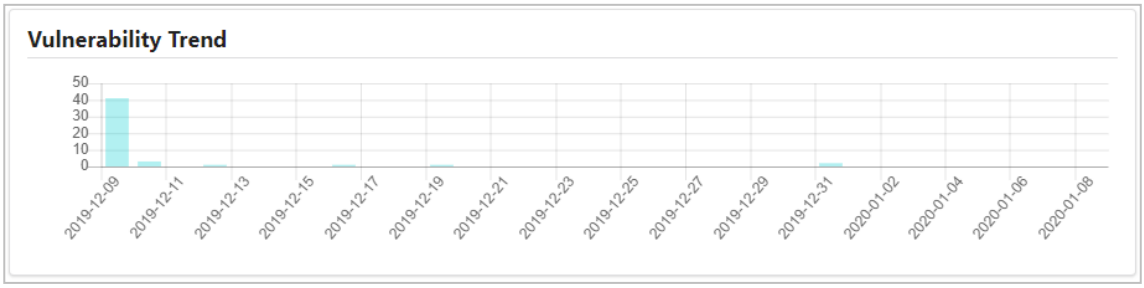
Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

Security Monitoring Center
Security Analysis Team

01. Overview

A vulnerability has been identified (CVE-2019-2890) that allows Oracle Fusion Middleware's WebLogic Server to bypass deserialization and execute remote commands through malicious T3 protocol requests with specific privileges. The vulnerability is caused by missing validation of input values during the deserialization process, which converts data converted to binary form back to the original form when receiving data from WebLogic Server.

The CVE list was released on October 16, 2019, and is included in the October 2019 Oracle Critical Patch Update list to complete the security patch.
The figure of the Vulnerability Trend of Vulmon (Vulnerability Intelligence Search Engine), which diagnoses CVE vulnerabilities, can be used to infer why an update advisory was issued.



[Figure 4-1] Search results for Cul-2019-2890 in Vulmon

Since the release of the vulnerability, more than 10 PoCs have been released on GitHub and the impact of the vulnerability is high. This issue details the CVE-2019-2890, a remote command execution vulnerability using the T3 protocol in WebLogic Server in Oracle Fusion Middleware. Let's look at it.

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

02. Vulnerability assessment

1) Affected Software

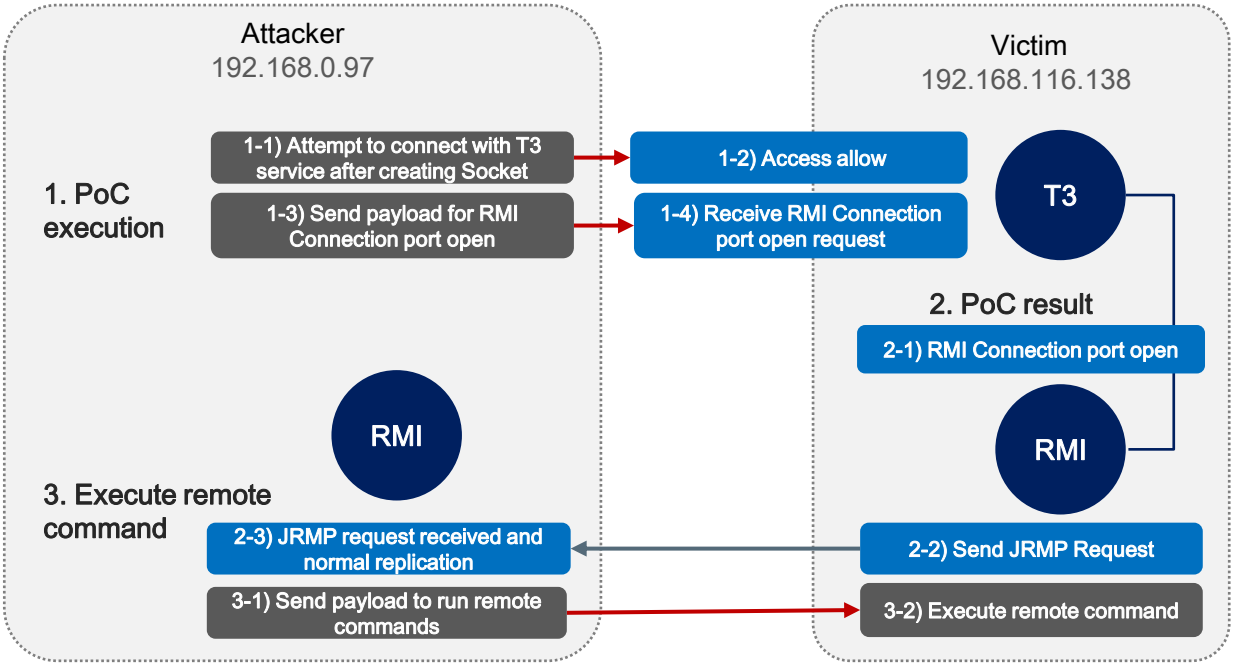
CVE	Vulnerability version	Risk level
CVE-2019-2890	WebLogic Server 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0	High

[Table 4-1] Version information of Affected by CVE-2019-2890

2) Vulnerability mechanism of CVE-2019-2890

When the WebLogic console is executed, the T3 protocol used for RMI (Remote Method Invocation) communication is activated to Default Port 7001, and data can be transferred between WebLogic Server and Client through the T3 protocol. CVE-2019-2890 remotely executes arbitrary commands through the Remote Method Invocation (RMI) connection, a technology that allows a Java program to call a method between each object and a computer after sending a command manipulated using the T3 protocol to a server. It is a vulnerability that is transmitted and executed.

The T3 protocol performs serialization in order to transmit data securely, and in case of receiving data, deserialization of converting data converted to binary data into original data is performed. The point where the vulnerability occurs is caused by the lack of verification of the input data during the deserialization process from the received data to the original data.



[Figure 4-2] CVE-2019-2890 Attack scenario

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

3) Detailed analysis of CVE-2019-2890

To understand the deserialization vulnerability of CVE-2019-2890, it is necessary to understand the serialization process of WebLogic Server. Serialization of WebLogic Server is implemented through weblogic.wsee.jaxws.persistence.PersistentContext.class in weblogic.jar file.

In order to serialize in WebLogic Server, as shown in [Figure 4-4], encryption is performed through EncryptionUtil.encrypt () using SerializedSystemIni.dat file, a file that manages key needed for encryption / decryption in writeSubject method. This is why Oracle classifies CVE-2019-2809 as a vulnerability that requires authentication.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2019-2890	Oracle WebLogic Server	Web Services	T3	No	7.2	Network	Low	High	None	Un-changed	High	High	High	10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0	

[Figure 4-3] Oracle Official Release – Vulnerability required authentication : CVE-2019-2890

```
private void writeSubject(ObjectOutputStream var1) throws IOException {
    ByteArrayOutputStream var2 = new ByteArrayOutputStream();
    ObjectOutputStream var3 = new ObjectOutputStream(var2);

    if (SubjectManager.getSubjectManager().isKernelIdentity(this._subject)) {
        AuthenticatedSubject var4 = (AuthenticatedSubject)SubjectManager.
        getSubjectManager().getAnonymousSubject();
        var3.writeObject(var4);
    } else {
        var3.writeObject(this._subject);
    }

    var3.flush();
    byte[] var5 = var2.toByteArray();

    if (KernelStatus.isServer()) {
        var5 = EncryptionUtil.encrypt(var5);
    }
    var5 = EncryptionUtil.encrypt(var5);

    var1.writeInt(var5.length);
    var1.write(var5);
}
```

▲ serialization

◀ encryption

[Figure 4-4] Serialization code in the writeSubject method

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

Serialized data generated by writeSubject method is transmitted to WebLogic Server through T3 protocol, and deserialization process can be executed through readObject method to execute arbitrary command.

```
private void readSubject(ObjectInputStream var1) {
    try {
        int var2 = var1.readInt();
        byte[] var3 = new byte[var2];
        var1.readFully(var3);
        if (KernelStatus.isServer()) {
            var3 = EncryptionUtil.decrypt(var3);
        }

        ByteArrayInputStream var4 = new ByteArrayInputStream(var3);
        ObjectInputStream var5 = new ObjectInputStream(var4);
        this._subject = (AuthenticatedSubject)var5.readObject();
    } catch (Exception var6) {
        WseeCoreLogger.logUnexpectedException("Couldn't completely read
        PersistentContext subject", var6);
    }

}
```

◂ Data read + decrypt

▾ deserialization

[Figure 4-5] deserialization code in the writeSubject method

4) PoC Analysis

When the PoC is executed, as described above, the payload transmitting the contents of opening the RMI connection port, which is a passage for remote command execution, is transmitted after communicating with the T3 service. This payload is created by referring to RMI related class and contains serializing RemoteObjectInvocationHandler after server-side RMI object activation and establishing TCP connection with remote end using UnicasfRef.

```
Object;xpw...x.....s}.....java.rmi.activation.Activatorxr..java.lang.reflect.Proxy.'. ..C....L..ht.%Ljava/lang/reflect/InvocationHandler;xpsr.-
java.rmi.server.RemoteObjectInvocationHandler.....xr..java.rmi.server.RemoteObject.a...a3....xpw7.
UnicastRef..192.168.0.97...Y.....x.....sr.
```

[Figure 4-6] Payload for RMI Connection port open

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

Class	Description
java.rmi.activation	Support for operating RMI objects
java.lang.reflect.Proxy	Provide static methods for creating dynamic proxy classes
java/lang/reflect/InvocationHandler	Interfaces Used by Java Remote Method Invocation (Java RMI)
java.rmi.server.RemoteObjectInvocationHandler	InvocationHandler interface implementation for use with Java Remote Method Invocation (Java RMI)
java.rmi.server.RemoteObject	Used to get stubs that communicate with remote objects by exporting them using JRMP
UnicastRef	1:1 communication method using destination's IP address as destination

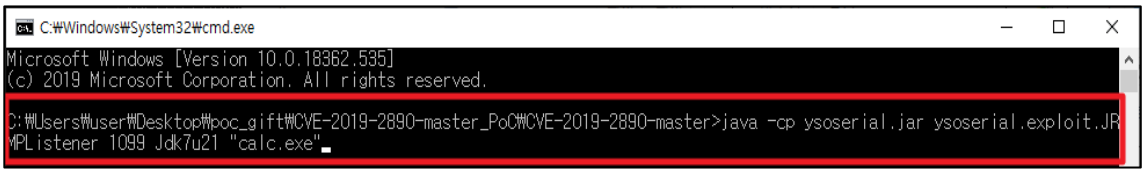
5) CVE-2019-2890 attack test

Information on environment construction for analysis and test is shown in [Table 4-3]

Attacker	Victim
Windows 10 192.168.0.97	Windows 7 (WebLogic 10.3.6.0) 192.168.116.138 : 7001

[Table 4-3] Testing environment

① The attacker opens the RMI Connection port (1099) using Ysoserial's JRMPListener library to perform an RCE attack..

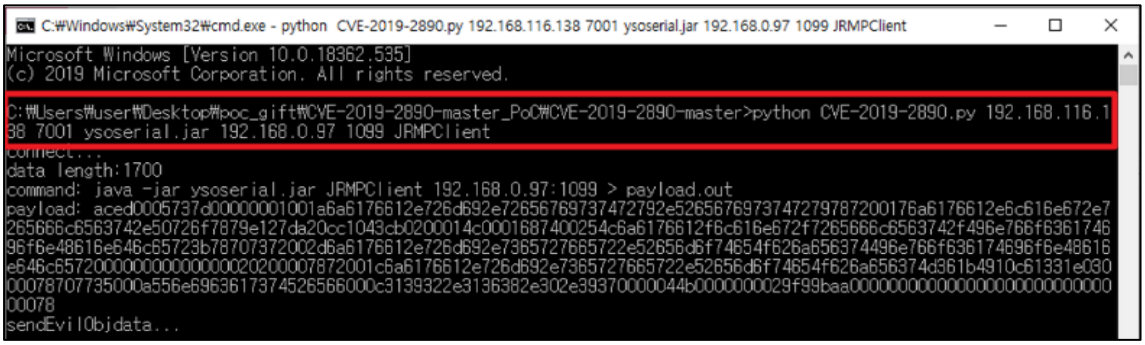


[Figure 4-7] Attacker RMI Connection port open

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

② PoC uses T3 protocol to transmit payload that opens WebLogic Server's RMI Connection port through socket communication.



[Figure 4-8] PoC Execution and Payload Transfer Screen

If the T3 protocol connection is successful, the transmission details of ConstantTransformer and InvokerTransformer included in the payload used for RMI connection of WebLogic Server can be checked through network packet as shown in [Figure 4-9].

[Figure 4-9] Payload Connection History for RCE Connection

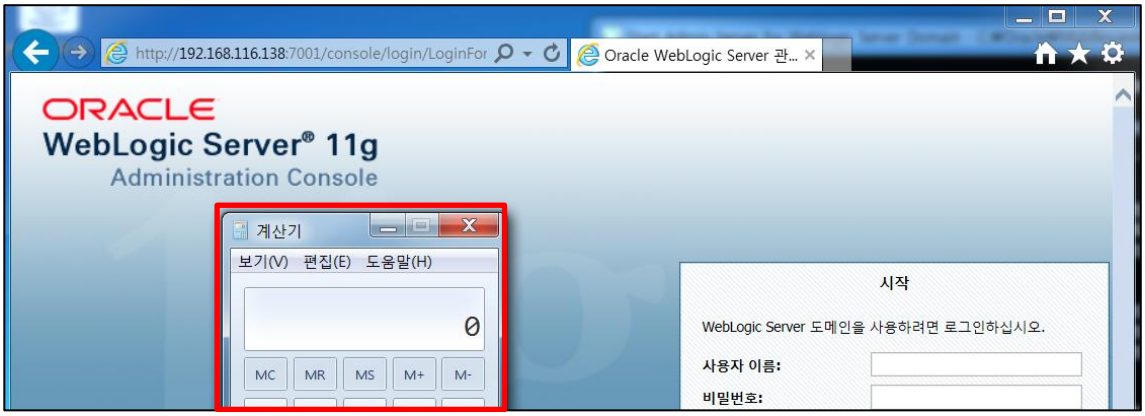
③ Send payload for remote command execution through RMI connection port 1099.

[Figure 4-10] Command execution log through the deserialization process

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

④ Verify remote command execution



[Figure 4-11] Calculator execution screen with RCE instruction

If the serialization of the RMI connection succeeds with the attack payload input by the attacker, the RMI connection port on the WebLogic Server side is opened. By sending a response code to the attacker through the Java Remote Method Protocol (JRPM), which allows objects in the JVM to call methods of objects running in other JVMs, the attacker can send arbitrary remote commands to Victim. .

[Figure 4-12] Execution history of arbitrary remote command majored in Attacker

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

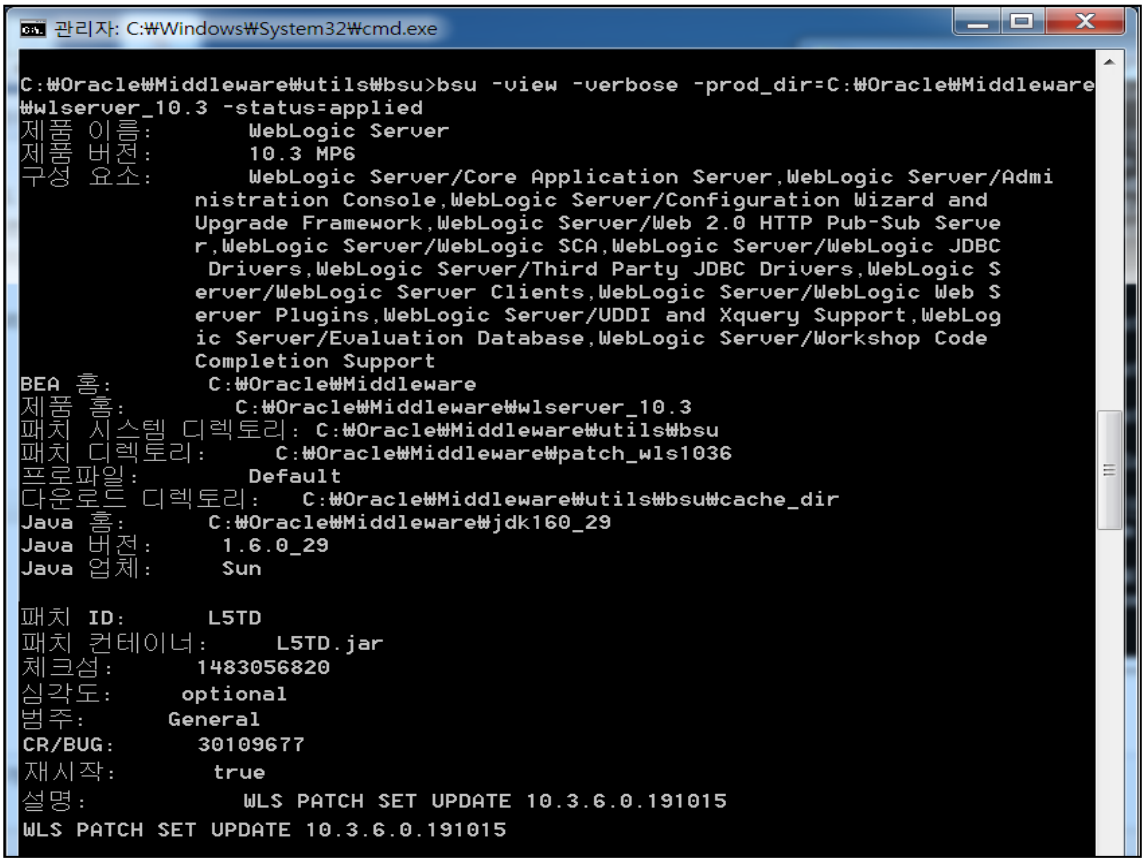
03. Countermeasure

1) WebLogic security patch apply

Vulnerable version	Secured version(latest version)
WebLogic Server 10.3.6.0	WebLogic Server 10.3.6.0.191015
WebLogic Server 12.1.3.0	WebLogic Server 12.1.3.0.191015
WebLogic Server 12.2.1.3	WebLogic Server 12.2.1.4

[Table 4-4] Secured WebLogic version to CVE-2019-2890

Versions below 12.1.1.0 of WebLogic Server can be checked through the bsu, print version command, and the Admin Console screen of WebLogic Server.



[Figure 4-13] Results of Checking WebLogic Version Information in WebLogic Server 10.3.6.0

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Oracle WebLogic RCE vulnerability(CVE-2019-2890) analysis and response

If you look at the source code before and after patching the vulnerability, you can see that the deserialization syntax in question in the readSubject method is validated using the WSFilteringObjectInputStream method. This method checks whether the object to be deserialized is a subclass of subject, otherwise terminates the deserialization process after an error occurs.

Classification	Revision history

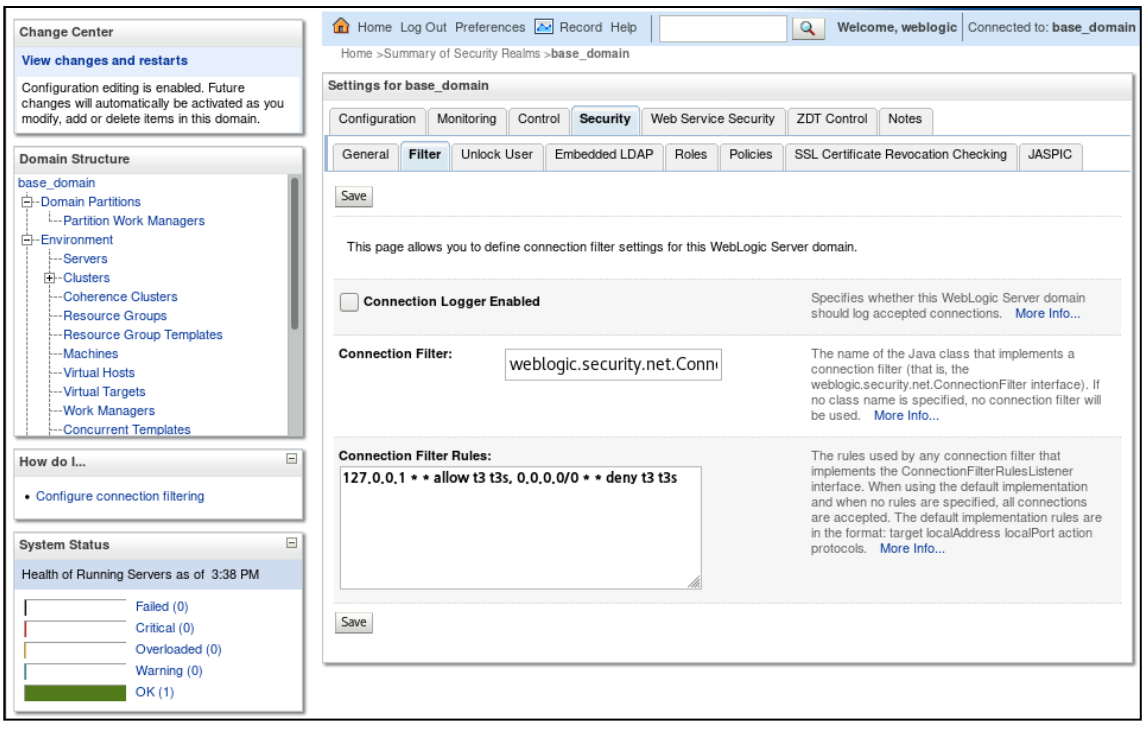
BEFORE (WebLogic Server 10.3.6.0)	`ByteArrayInputStream var4 = new ByteArrayInputStream(var3);`
	`ObjectInputStream var5 = new ObjectInputStream(var4);`
	`this._subject = (AuthenticatedSubject)var5.readObject();`

AFTER (WebLogic Server 10.3.6.0.191015)	`ByteArrayInputStream var4 = new ByteArrayInputStream(var3);`
	`ObjectInputStream var5 = new PersistentContext.WSFilteringObjectInputStream(var4);`
	`this._subject = (AuthenticatedSubject)var5.readObject();`

[Table 4-5] WebLogic Vulnerability Source Code Security Patch Comparison

2) T3 Protocol deactivation

Because Oracle WebLogic uses the T3 protocol for all connections except HTTP communication, system impact is high, but it is possible to respond by temporarily disabling the T3 protocol.



[Figure 4-14] Apply T3 Protocol Block within WebLogic Server screen

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1) WebLogic console open 2) Configure filters by clicking [Filter] within the [Security] tab on the Base_domain configuration page - Connection Filter item : weblogic.security.net.ConnectionFilterImpl - Connection Filter Rules item : 127.0.0.1 * * allow t3 t3s, 0.0.0.0/0 * * deny t3 t3s 3) save (no need restart)

[Table 4-6] How to block T3 protocol within WebLogic Server

04. Reference

[1] Oracle WebLogic Server Remote Code Execution Security Update Advisory (2019.12.09)
https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=35222
https://www.oracle.com/security-alerts/cpuoct2019.html
[2] CVE-2019-2890 PoC
https://github.com/ZO1RO/CVE-2019-2890
https://github.com/SukaraLin/CVE-2019-2890
[3] WebLogic RCE (CVE-2019-2890) Debug Diary
https://paper.seebug.org/1069/
[4] WebLogic t3 Deserialization Vulnerability-CVE-2019-2890
http://gv7.me/articles/2019/cve-2019-2890-vulnerability-analysis/
[5] Proof-of-concept tool for generating payloads using insecure Java object deserialization
https://github.com/frohoff/ysoserial
[6] Java Method Articles
http://cris.joongbu.ac.kr/course/java/api/java/rmi/activation/Activator.html
http://cris.joongbu.ac.kr/course/2018-1/jcp/api/java/rmi/server/class-use/RemoteObject.html
[7] Latest version of Oracle
https://blogs.oracle.com/fusionmiddlewaresupport/october-2019-oracle-weblogic-server-patch-set-update-have-been-released

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

CHAPTER 5

Focus On IGLOO Security

1. IGLOO SECURITY selected as '2020 Youth-Friendly Enterprise'

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Focus on IGLOO Security

IGLOO SECURITY selected as '2020 Youth-Friendly Enterprise

'2020 Youth-Friendly Enterprise

- Efforts to increase youth employment and create a work environment for work-life balance were recognized.

[23rd December 2019] IGLOO SECURITY Co., Ltd. (CEO Lee Deuk-Choon, www.igloosec.co.kr/en) announced on the 23rd that it was selected as '2020 Youth-Friendly Enterprise' hosted by the Ministry of Employment and Labor. Youth-friendly enterprises are companies that high-quality firms with high employment stability and work-life balance for young staffs.

IGLOO SECURITY was highly regarded for creating quality jobs for young workers. IGLOO SECURITY hired over 70% of its recruits to young people, and recruited more than 30% of its employees as local talents through its linked recruitment program. In addition, the company has run an in-house training program, “Igloo School,” which can range from beginner security personnel to skilled professionals.

In addition, the improvement of personnel and welfare system in line with job characteristics also received good scores. Igloo Security has been working to balance work and life by encouraging flexible working and flexible working according to the job, encouraging annual use during the opening of the bridge. In addition, It has been at the forefront of creating an enjoyable workplace by hosting “Igloo Lotto” events to recruit overseas volunteers and “Igloo Brownback” meetings where they discusses their job while eating sandwiches.

Mr. Lee (the CEO of IGLOO SECURITY) said that “I believe that the best way for companies to contribute to society is to find young talents and create high-quality jobs and We will continue to work hard to balance work and life and to make a leap with the company.”

Copyright © IGLOO Security, Inc. 2020. All rights reserved.

We Know SECURITY!

Published by IGLOO SECURITY (www.igloosec.co.kr)
6 Floor. 7, Jeongui-ro 8-gil, Songpa-gu, Seoul, Korea
T. +82-2-3404-8678
E-mail. overseas@igloosec.com

Distributed by Cyber-Infinity Corp. (www.ci-corp.jp)
株式会社 シーアイシー
東京都千代田区岩本町3-4-3 リードシー秋葉原ビル5階
T. +81-3-5829-5801
E-mail. business@ci-corp.jp

Edited by IGLOO SECURITY Marketing Team
Translated by IGLOO SECURITY Overseas Business Team
© 2020 IGLOO SECURITY, Inc. All rights reserved.
The copyright of this publication is held by IGLOO SECURITY. It is not permissible to reproduce, copy, or distribute any or all of the contents of this publication in any form or by any means without the prior written consent of IGLOO SECURITY. All information contained in the publication can be changed without prior notice.