PIOLINK

중국 국가 후원 조직이 악용하는

취약점 리스트

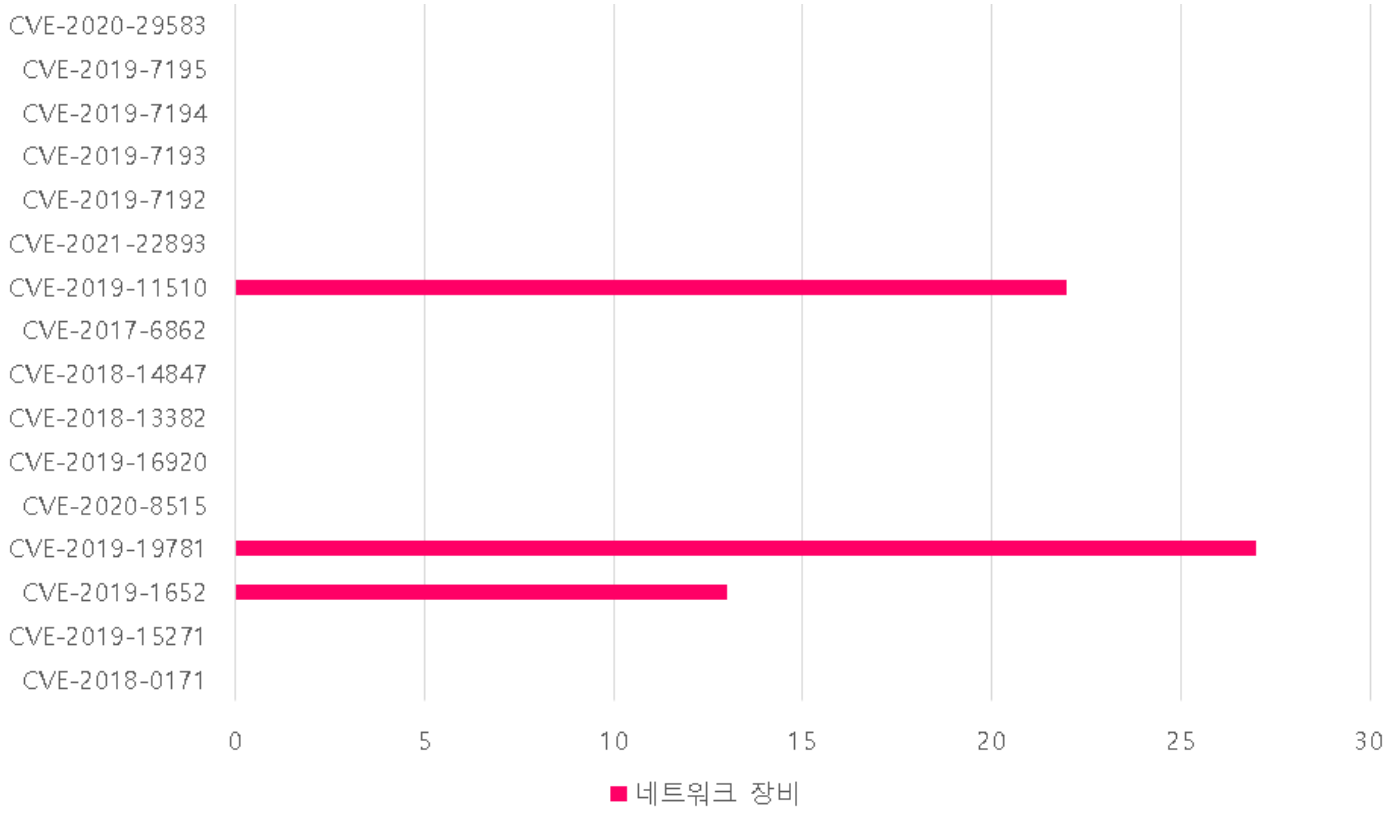
미국 국토안보부 산하기관인 사이버보안 및 인프라 보안국(이하 CISA)은 지난 7일 NSA와 FBI와 함께 중국 국가의 후원을 받는 사이버 조직이 통신 및 네트워크 서비스 공급업체의 제품을 대상으로 악용하는 취약점 리스트를 발표하였다.

[표] 중국 정부가 후원하는 사이버 조직이 악용하는 네트워크 장치 및 취약점

공급업체	CVE	취약점 유형
Cisco	CVE-2018-0171	RCE
	CVE-2019-15271	RCE
	CVE-2019-1652	RCE
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	인증 우회
MikroTik	CVE-2018-14847	인증 우회
Netgear	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	인증 우회
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	권한 상승
	CVE-2019-7193	원격 주입
	CVE-2019-7194	XML 라우팅 우회 공격
	CVE-2019-7195	XML 라우팅 우회 공격
Zyxel	CVE-2020-29583	인증 우회

사이버 공격 조직들은 통신 및 네트워크 서비스를 제공하는 기업의 제품을 표적으로 삼아 정찰 및 취약점 검색을 수행하게 되는데 이 때, RouterScan/RouterSploit 와 같은 오픈 소스를 주로 사용한다. 네트워크 장치 및 해당 장치의 취약점을 스캔하기 위해 RouterScan 도구를 사용하며, 익스플로잇 프레임워크인 도구를 사용하여 대상 기기에 실제 익스플로잇을 수행한다. 위 표에 나온 공급업체 제품들을 대상으로 손쉽게 익스플로잇 할 수 있게 도와주는 도구들인 것이다.

파이오링크 침해대응센터에서는 사이버 위협 인텔리전스를 통해 국내에 취약한 네트워크 장치를 검색하여 얼마나 존재하는지 확인해 보았다.



<그림> 국내 취약 네트워크 장비

CVE-2019-1652 취약점을 가진 시스코 라우터 장비는 총 13대, CVE-2019-19781 취약점을 가진 시트릭스 장비는 27대, CVE-2019-11510 취약점을 가진 Pulse VPN 장비는 22대로 확인되었다.

국내에서 확인된 3가지 취약점에 대해 간단히 살펴보면 다음과 같다.

Cisco CVE-2019-1652 CVSS 3.0: 7.2(높음)	
취약점 설명	Cisco Small Business RV320 및 RV325 Dual Gigabit WAN VPN Routers의 웹 기반 관리 인터페이스에 취약성이 있으며 이를 통해 영향을 받는 장치에 대한 관리 권한을 가진 인증된 원격 공격자가 임의 명령을 실행할 수 있다. 이 취약성은 사용자 제공 입력의 잘못된 유효성 검사로 인해 발생한다. 공격자는 악의적인 HTTP POST 요청을 영향을 받는 장치의 웹 기반 관리 인터페이스에 전송하여 이 취약성을 이용할 수 있다. 공격이 성공하면 공격자가 기본 Linux 쉘에서 임의 명령을 루트로 실행할 수 있다. Cisco는 이 취약성을 해결하는 펌웨어 업데이트를 릴리스하였다.
대응방법	펌웨어 버전 1.4.2.22 이상으로 업데이트 원격 관리 기능을 사용하도록 설정한 경우 노출을 줄이기 위해 사용하지 않도록 설정
탐지방법	N/A
취약버전	펌웨어 버전 1.4.2.15 ~ 1.4.2.20 를 사용하는 Cisco Small Business RV320 및 RV325 Dual Gigabit WAN VPN Routers

시트릭스 CVE-2019-19781 CVSS 3.0: 9.8(중요)	
취약점 설명	Citrix ADC(Application Delivery Controller) 및 Gateway 10.5, 11.1, 12.0, 12.1 및 13.0에서 문제가 발견되었다. 디렉토리 트래버설을 허용한다.

대응방법	https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance
탐지방법	https://support.citrix.com/article/CTX269180
취약버전	다음 Citrix 제품 버전에 영향 Citrix ADC and Citrix Gateway 13.0.47.24 이전 NetScaler ADC 및 NetScaler Gateway 12.1.55.18 이전 NetScaler ADC 및 NetScaler Gateway 12.0.63.13 이전 NetScaler ADC 및 NetScaler Gateway 11.1.63.15 이전 NetScaler ADC 및 NetScaler Gateway 10.5.70.12 이전 Citrix SD-WAN WANOP 어플라이언스 모델 4000-WO, 4100-WO, 5000-WO 및 5100-WO 10.2.6b 및 11.0.3b 이전

Pulse CVE-2019-11510 CVSS 3.0: 10(중요)	
취약점 설명	Pulse Secure PCS(Pulse Connect Secure) 8.2(8.2R12.1 이전), 8.3(8.3R7.1 이전), 9.0(9.0R3.4 이전)에서 인증되지 않은 원격 공격자는 특수하게 조작된 URI를 보내 임의 파일 읽기 취약점을 수행할 수 있다.
대응방법	Pulse Secure VPN 취약버전 이상으로 업그레이드
탐지방법	https://github.com/cisagov/check-your-pulse
취약버전	다음 Pulse Connect Secure 제품 버전에 영향 9.0R1 ~ 9.0R3.3 8.3R1 ~ 8.3R7 8.2R1 ~ 8.2R12

위에서 언급한 취약점들은 원격 코드 실행, 인증 우회 등으로 공격자가 언제든 기업 내부에 침투가 가능한 상태임을 나타낸다.

다른 취약점과는 달리, CVE-2019-11510 취약점을 가진 Pulse VPN 장비는 SSL 인증서를 통해 해당 장비를 사용중인 기업의 이름을 특정할 수 있었다. OO그룹, OO병원, OO가구, OO치킨, OO인증, OO제약, OO테크 등 대기업부터 중소기업까지 다양했다. 임의 파일 읽기 취약점을 통해 VPN 네트워크에 접근할 수 있기 때문에 랜섬웨어 감염 등 2차 공격으로 이어질 수 있다.

파이오링크 침해대응센터는 사이버 위협 인텔리전스 서비스 및 보안 예방 활동을 통해 자사 고객의 자산을 보호하고 있다.

참고자료

https://www.cisa.gov/uscert/ncas/alerts/aa22-158a