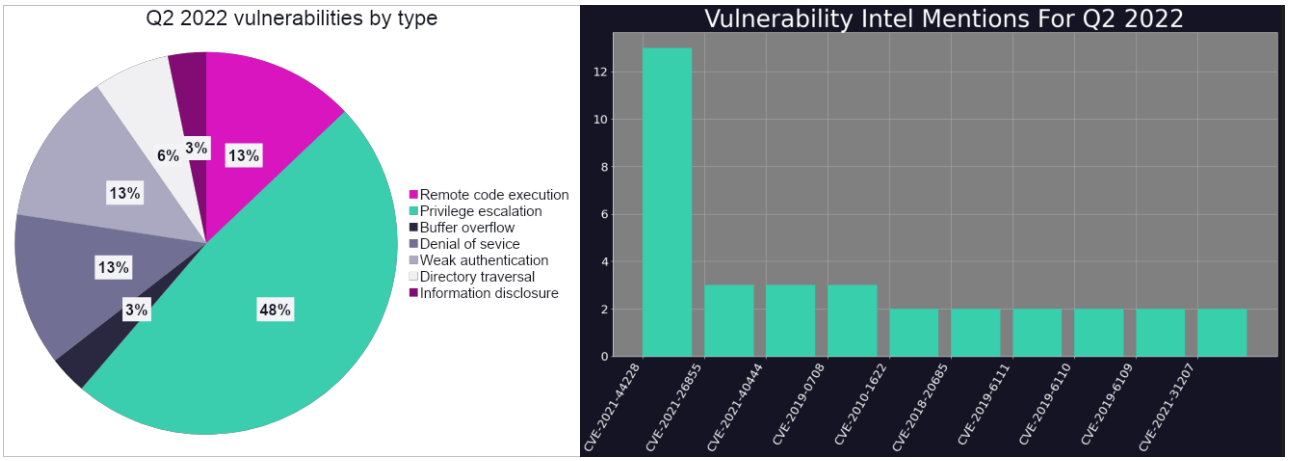
PIOLINK

22.02 분기 취약점 정리

국내 현황은?

1. Q2.22 취약점 현황

권한 상승 취약점은 22년 2분기에 가장 많이 악용된 취약점으로, 보고된 사고의 48%를 나타낸다. 그 다음으로 취약한 인증, 원격 코드 실행(RCE), 서비스 거부 공격(DoS) 취약점이 각각 13%로 나타났다.(그림(좌))

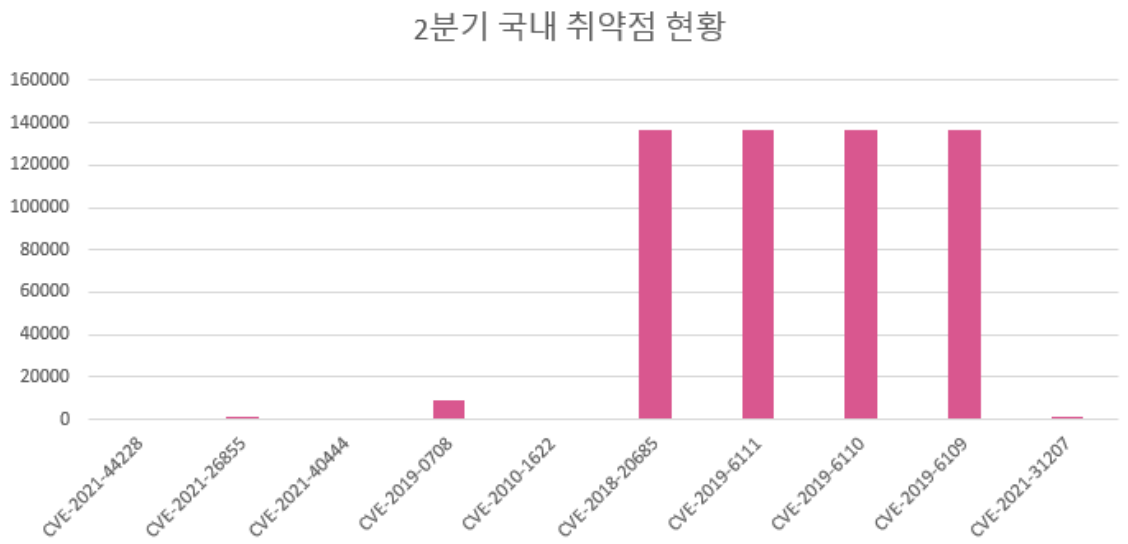


<그림> 2분기 악용된 취약점 유형(좌), CTI에서 언급된 취약점 순(우) 출처: digitalshadows blog

인텔리전스에서 가장 많이 언급된 취약점은 Log4Shell 취약점이다. Log4Shell(CVE-2021-44228) 취약점은 트윗, 붙여넣기, 블로그, 웹 페이지, 인터넷 릴레이 채팅 및 Github를 포함한 광범위한 소스에서 가장 많이 논의된 취약점이다. 최근 동향을 보면 위협 조직들이 계속해서 많은 수의 Log4Shell 취약점을 노리는 것이 확인되었다. 그 다음 취약점으로는 ProxyLogon 취약점(CVE-2021-26855), Microsoft HTML에 영향을 미치는 RCE 취약점(MSHTML – CVE-2021-40444) 및 BlueKeep RDP(CVE-2019-0708) 취약점이 뒤를 따랐다. 놀라운 점은 Java 어플리케이션을 위한 오픈 소스 프레임워크인 SpringSource에 영향을 미치는 2010년 취약점이 포함되어 있다는 점이다. 이 취약점은 2022년에 발표된 Spring4Shell(CVE-2022-22965) 취약점과 관련이 있다. Spring4Shell 취약점은 CVE-2010-1622 취약점 패치를 우회하여 악용되기 때문이다.

2. 국내 현황은?

2분기에 악용된 취약점을 중심으로 국내 현황을 살펴보았다.



<그림> 2분기 취약점 기준 국내 현황

특정 환경에서의 취약점 확인(CVE-2021-44228) 및 외부에서 확인이 불가한 MSHTML을 사용하는 어플리케이션 취약점(CVE-2021-40444)을 제외하면 2분기에 이슈가 되었던 취약점 모두 국내에 존재하는 것으로 확인되었다. CVE-2021-26855 취약점은 마이크로소프트사의 Exchange 서버에서 발생하는 취약점으로 SSRF 공격을 통해 사용자 인증 없이 인증된 사용자 권한을 획득할 수 있는 취약점이다. 이 취약점이 성공하게 되면, CVE-2021-27065와 같은 취약점을 통해 웹 쉘을 업로드할 수 있게 된다. 국내에 취약한 서버는 총 50여대로 확인되었다. 취약한 서버를 살펴보면, OO홀딩스, OO무역, OO출판, OO대학교, OO그룹, OO법무법인, OO병원 등 다양한 기관, 기업이 확인되었고, 자동차 반도체 기업, 화학제품, 태양광 발전 기업들도 포함되었다.

[표] 2분기 취약점 기준 국내 현황표

취약점	설명	국내취약서버
CVE-2021-44228	Log4Shell 취약점	0
CVE-2021-26855	ProxyLogon 취약점	51
CVE-2021-40444	MSHTML RCE취약점	0
CVE-2019-0708	BlueKeep RDP	8600
CVE-2010-1622	Spring 취약점	0
CVE-2018-20685	SCP 프로토콜 취약점	136938
CVE-2019-6111	SCP 권한상승	136938
CVE-2019-6110	SCP 프로토콜 취약점	136937
CVE-2019-6109	SCP 클라이언트 스푸핑	136939
CVE-2021-31207	MS Exchange Server ProxyShell 취약점	141

CVE-2019-0708 BlueKeep 취약점은 윈도우 원격 데스크톱 서비스를 이용해 정상적인 인증 단계 필요없이 원격에서 임의의 코드를 실행할 수 있는 취약점이다. 해당 취약점을 이용해 랜섬웨어 등 악성코드를 실행할 수 있는 가능성이 있음으로 상당한 주의가 필요한 취약점이다. 국내 취약 시스템은 총 8600여대로 확인된다.

SCP 프로토콜 관련 취약점 4개(CVE-2018-20685, CVE-2019-6111, CVE-2019-6110, CVE-2019-6109)의 경우 악의적인 코드를 실행하거나, 권한상승, 스푸핑 등을 수행할 수 있는 취약점으로 국내 확인된 취약 시스템은 총 13만 7천여대로 확인되었다.

CVE-2021-31207 ProxyShell 취약점은 마이크로소프트 Exchange 서버에서 발생하는 취약점으로 보안기능을 우회할 수 있으며, CVE-2021-34473(원격코드 실행), CVE-2021-34523(권한상승) 취약점과 함께 공격이 가능하다. 국내 취약한 시스템은 140여대로 메모리 팹리스 기업, 교육 컨텐츠, OO홀딩스, OO대학교, OO반도체, OO그룹 등이 취약한 것으로 확인되었다.

3. 마무리

이슈가 되는 취약점들은 그 만큼 취약한 시스템이 많다는 것을 반증한다. 이러한 취약점들은 제조사의 최신 업데이트만이라도 꾸준히 적용한다면 사전에 대응할 수 있는 것들이다. 기본을 지키는 것이 보안사고를 막을 수 있는 지름길이다. 파이오링크 침해대응센터에서는 이러한 보안예방활동을 통해 사이버 위협으로부터 자사 고객사들의 자산을 보호하고 있다.