PIOLINK

보안위협분석

현재 활발하게 악용되는 취약점

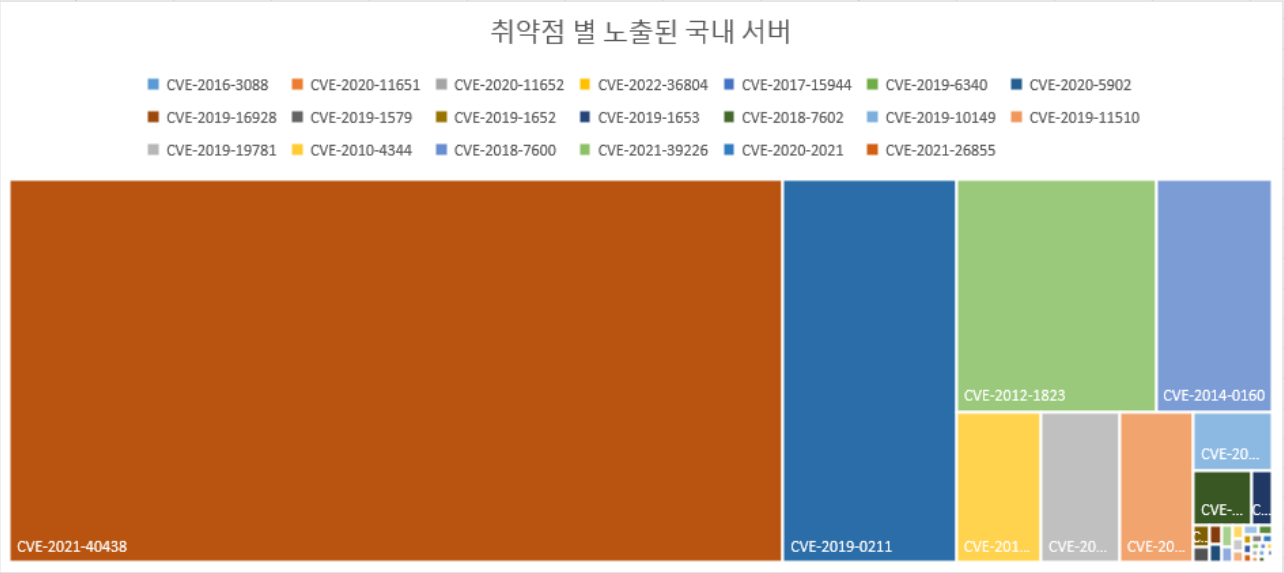
국내 현황은?

2023년 2월 9일

㈜파이오링크 사이버위협분석팀

미 CISA는 활발하게 악용되는 것으로 알려진 취약점 목록을 공개한다. Know Exploited Vulnerabilities 라고 불리우는 이 취약점 목록에는 870여개의 취약점이 포함되어 있다. 우리는 인텔리전스 기반으로 국내에 해당 취약점이 노출된 시스템이 얼마나 되는지 알아보기로 하였다.

인텔리전스 기반 통계 분석



〈그림〉 취약점 별 노출된 국내 서버 비중

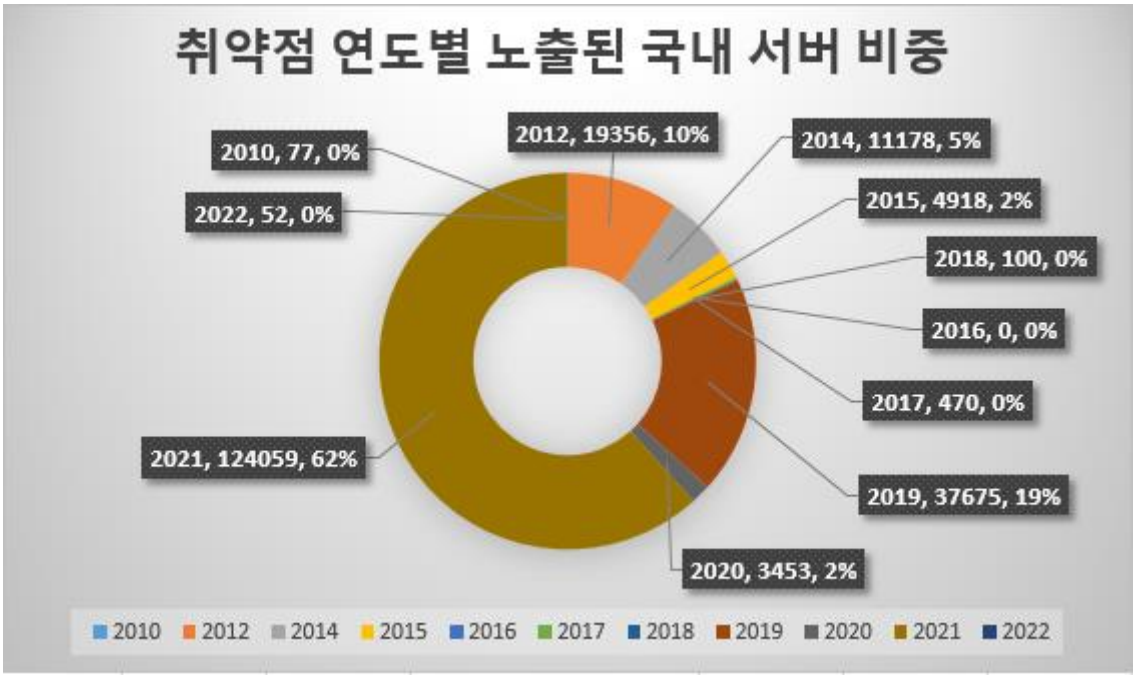
우리는 먼저 870여개 취약점을 대상으로 인텔리전스에서 식별가능한 취약점을 확인 해 보았다. 인텔리전스의 경우 대부분의 취약점 점검이 앱 버전 및 기타 수동/커스터마이징 방법을 통해 이루어지기 때문에 식별가능한 취약점이 제한된다. 인텔리전스 확인 결과 취약점 870여개 중 44개의 취약점을 식별할 수 있었다.

[표] 국내 취약 서버 취약점 TOP 10

취약점	설명	국내 취약 서버 (대)
CVE-2021-40438	Apache 취약점	123,385
CVE-2019-0211	Apache 취약점	27,647
CVE-2012-1823	PHP 취약점	19,356
CVE-2014-0160	OpenSSL Heartbleed	11,178

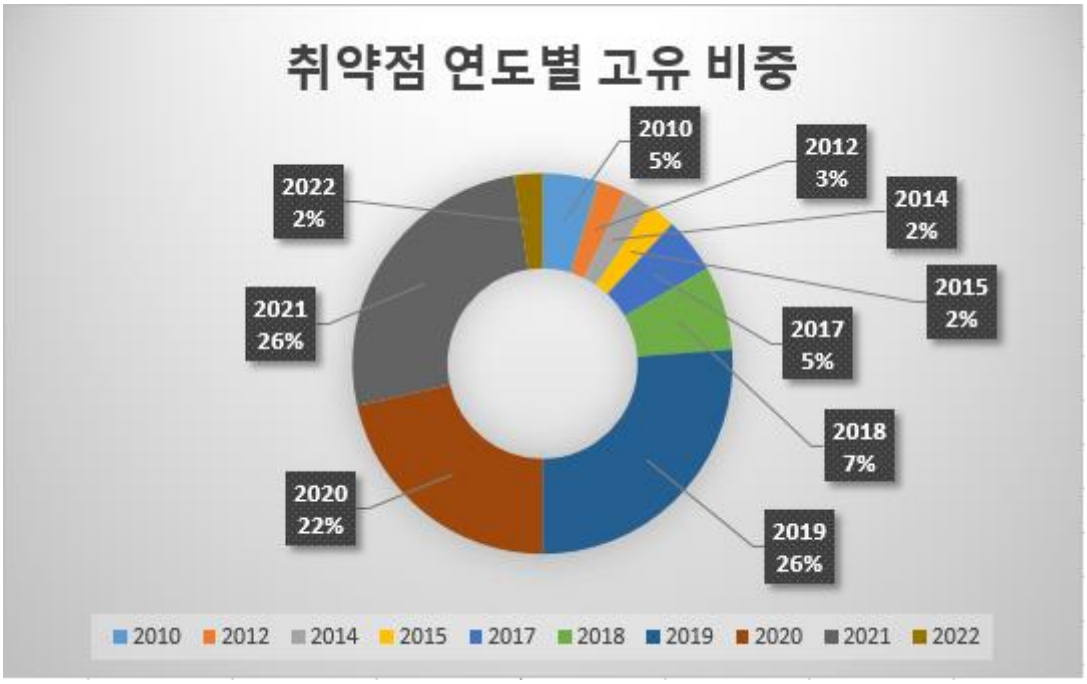
CVE-2019-11043	PHP 취약점	5,319
CVE-2015-1635	IIS 취약점	4,918
CVE-2019-0708	BlueKeep RDP	4,630
CVE-2020-0796	SMB 취약점	1,907
CVE-2020-1938	Apache 취약점	1,341
CVE-2017-7269	IIS6.0 취약점	468

44개 취약점 중 CVE-2021-40438 이 123,385대로 가장 많았으며, CVE-2019-0211 과 CVE-2012-1823 취약점이 각각 27647대, 19,356대로 그 뒤를 따랐다.



〈그림〉 취약점 연도별 노출된 국내 서버 비중

취약점 연도별로 살펴보면 2021년 발생한 취약점에 노출된 시스템이 62%로 가장 많았으며, 그 뒤를 이어 2019년도 취약점이 19%, 2012년도 취약점이 10%를 차지했다. 나온 지 1~2년이 지난 취약점들에 대한 대응이 가장 안 이루어졌으며, 10년도 지난 2012년도 취약점이 10% 차지한다는 것은 보안에 얼마나 취약한지를 보여주는 대목이다.



〈그림〉 취약점 연도별 고유 비중

연도별로 나온 취약점을 살펴보면, 2019년도와 2021년도 취약점이 각각 11개로 26%를 차지했으며, 2020년도 취약점이 9개(22%)로 그 뒤를 따랐다.

취약점 분석 통계

우리는 국내에 취약 서버가 많은 순서대로 취약점 TOP10을 선정하여 분석하였다.

[표] 취약점 TOP 10

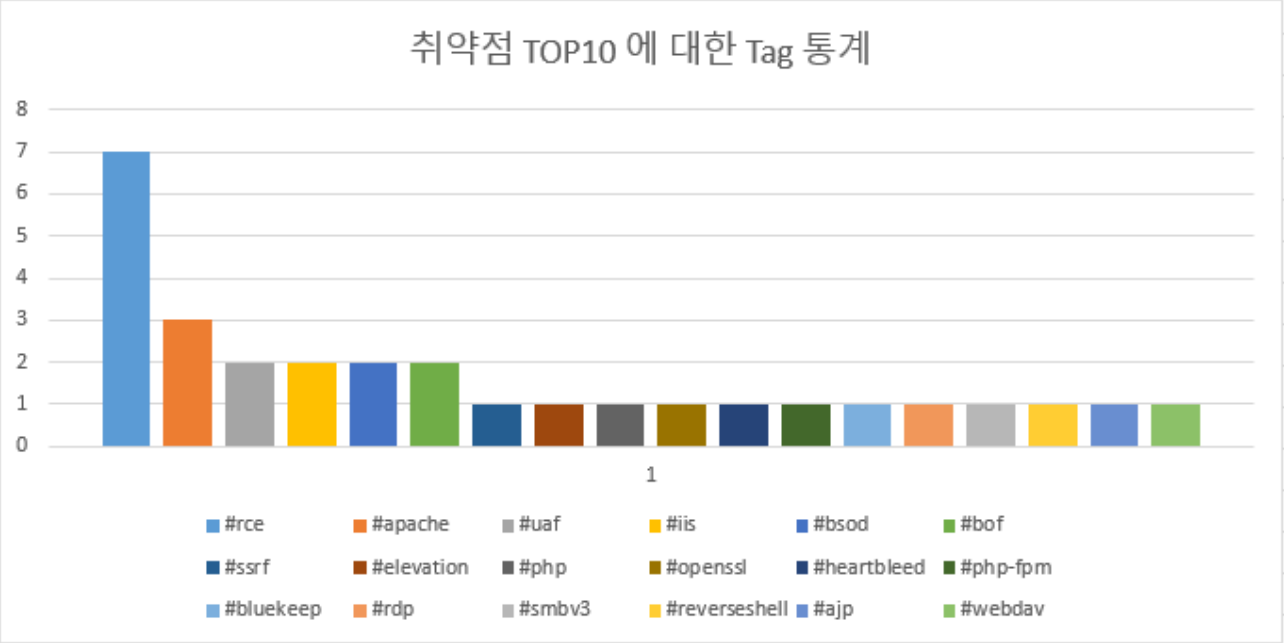
CVE	CVSSv3	Tag	Condition
CVE-2021-40438	9.0	#ssrf #apache	Apache HTTP Server2.4.48 이전 모든버전 (mod_proxy 활성화)
CVE-2019-0211	7.8	#uaf #apache #elevation	Apache HTTP Server 2.4.17~2.4.38 버전
CVE-2012-1823	n/a	#rce #php	PHP 5.3.12 이전 버전 PHP 5.4.2 이전 버전

CVE-2014-0160	7.5	#openssl #heartbleed	OpenSSL 1.0.1 ~ OpenSSL 1.0.1f OpenSSL 1.0.2-beta OpenSSL 1.0.2-beta1
CVE-2019-11043	8.7	#rce #php-fpm	PHP FPM 7.1.x ~ 7.1.33 PHP FPM 7.2.x ~ 7.2.24 PHP FPM 7.3.x ~ 7.3.11
CVE-2015-1635	n/a	#rce #iis #bsod	Microsoft Windows 7 SP1 Windows Server 2008 R2 SP1 Windows 8, 8.1 Windows Server 2012 Gold and R2
CVE-2019-0708	9.8	#rce #bluekeep #rdp #bsod #uaf	Windows XP Windows 7 Windows Server 2003 Windows Server 2008 및 2008 R2
CVE-2020-0796	10.0	#rce #smbv3 #bof #reverseshell	Windows 10 (1903, 1909) Windows Server 2016 (1903, 1909)
CVE-2020-1938	9.8	#apache #ajp #rce	Apache Tomcat 6.x Apache Tomcat 7.0.0~7.0.99 Apache Tomcat 8.5.0~8.5.50 Apache Tomcat 9.0.0M1~9.0.30
CVE-2017-7269	9.8	#iis60 #webdav #rce #bof	IIS6.0 in Windows Server 2003 R2 x86

활발하게 활용되는 취약점들로 CVSSv3 점수 최소 7.5점 이상으로 이루어져 있으며, 대부분 9점 이상으로 분류된 취약점들임을 알 수 있다.

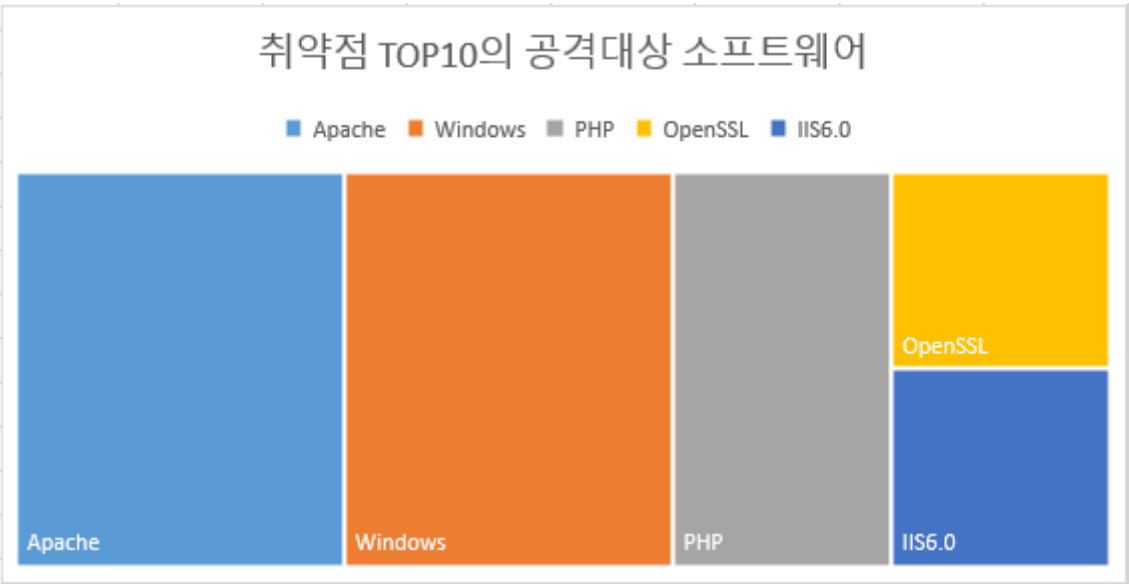
취약점들은 모두 인터넷에 POC 코드가 오픈되어 있어 누구라도 쉽게 공격 수행이 가능하며, POC 코드를 기반으로 악의적인 코딩이 가능한 상태이다. 일반적으로 신규 취약점으로 릴리즈가 되더라도 POC코드가 오

픈되지 않으면 피해가 거의 일어나지 않지만, 오픈이 되고 나면 패치되지 않은 서버를 중심으로 피해가 커지기 마련이다.



〈그림〉 취약점 TOP10의 Tag 정보

취약점 TOP10에 대한 Tag 정보를 기반으로 통계를 내 보면 예상대로 파급도가 큰 원격코드실행 취약점이 주를 이루었고 apache, UAF, IIS, BSOD, BOF 가 그 뒤를 따랐다.



〈그림〉 취약점 TOP10의 공격대상 소프트웨어

공격대상 소프트웨어의 경우 apache, windows 가 가장 많았고, PHP, OpenSSL, IIS6.0 순이었다.

마무리

지금까지 미 CISA에서 공개하는 KEV 데이터베이스 기반 국내 취약 서버 및 취약점들에 대해서 알아보았다. 인텔리전스를 분석하는 동안 우리는 국내 취약 서버들을 운영하고 있는 기관, 기업명의 이름들을 확인할 수 있었다. 이 과정에서 우리는 생각치도 못한, 보안이 잘 되어 있을 곳이라 생각했던 곳에서도 취약 서버가 있다는 사실을 알고 놀라움을 금치 못했다. 물론 우리는 인텔리전스에서 제공하는 국내 취약 서버들이 모두 취약하다고 생각하지 않는다. 앞서 언급했듯이 인텔리전스는 서비스 앱 버전, 수동/커스터마이징된 기법으로 취약점을 판단하고 있으며, 또한, 패치했다하더라도 버전은 변경되지 않는 경우도 있기 때문이다. 설령 취약한 서버라 하더라도 WAF와 같은 보안솔루션이 구축되어 있다면 실제 공격이 유효하지 않을 수도 있는 경우도 배제할 수 없기 때문이다. 그렇다 하더라도 수만~수십만 대의 취약서버 검색 결과는 시사하는 바가 크다. 그 중 취약 서버가 존재한다는 것은 부인할 수 없는 사실이기 때문이다.

우리가 알아 본 취약점들은 공격자들이 적극적으로 악용하는 취약점이기 때문에 인터넷에 노출되어 있는 시스템의 경우 빠르게 조치하는 것이 필요하다. 파이오링크 사이버위협분석팀에서는 이러한 인텔리전스 분석을 통해 자사 고객의 위협을 사전에 예방하는 활동을 수행하고 있으며, 주기적으로 고객사의 취약점 점검을 수행하여 침해사고가 발생하지 않도록 취약점 점검 서비스를 제공하고 있다.