|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 코스콤 금융클라우드 | | | | | | | |
| SECURITY MONITORING | | | | | | | |
| **한화생명 (채널계서비스(PRD))** | | | | | | | |
| Monthly Report | | | | | | | |
|  |  |  |  |  |  |  |  |
| 2024 년 08 월(2024-08-01 - 2024-08-31) | | | | | | | |
| Advanced Service | | | | | | | |
|  |  |  |  |  |  |  |  |
| **종합 관제 의견** | | | | | | | |
| 종합의견 | | 취약페이지 접근, 취약점을 악용한 시스템 명령 실행 시도 및 서버 정보 수집을 위한 스캔시도가 발생하였습니다.  보안장비에서 다수 차단되었고 추가 공격에 대비하여 공격자 IP를 임시 차단하였으나, 내부 시스템 영향도 파악을 위해 시스템 상태 및 로그 등의 확인이 필요합니다. 또한 내부 시스템에서 불필요 서비스 제거, 최신 버전 패치, 관리자페이지 접속 제한 및 계정 보안성 강화 등의 보안 설정을 권고드립니다. | | | | | |
| Anti-DDoS 대응 의견 | | 특이사항 없습니다. | | | | | |
| 웹방화벽 대응 의견 | | 취약페이지 접근, 정보수집을 위한 스캐닝 시도 및 취약점을 이용한 원격코드 실행 시도가 확인되었습니다.  공격 IP를 임시 차단하였습니다.  현재 설정된 최소 허용 TLS버전 1.1은 프로토콜 취약점을 이용한 다양한 공격에 노출될 수 있습니다. TLSv1.2 이상 설정 적용을 권고드립니다. | | | | | |
| IDS 대응 의견 | | 특이사항 없습니다. | | | | | |
| IPS 대응 의견 | | 취약 페이지 접근 시도 및 취약점을 이용한 원격코드 실행 시도가 확인되었습니다.  공격 IP를 임시 차단하였습니다. | | | | | |
|  |  |  |  |  |  |  |  |
| **보안장비별 보호 대상 서버** | | | | | | | |
| **Anti-DDoS** | | **웹방화벽** | | **IDS** | | **IPS** | |
| 39.125.131.76  112.172.179.93  112.172.179.92  112.172.179.91  112.172.179.90  112.172.179.89  112.172.179.102  112.172.179.94 | | 39.125.131.76  112.172.179.93  112.172.179.92  112.172.179.91  112.172.179.90  112.172.179.89  112.172.179.102  112.172.179.94 | | 39.125.131.76  112.172.179.93  112.172.179.92  112.172.179.91  112.172.179.90  112.172.179.89  112.172.179.102  112.172.179.94 | | 39.125.131.76  112.172.179.93  112.172.179.92  112.172.179.91  112.172.179.90  112.172.179.89  112.172.179.102  112.172.179.94 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **보안장비별 공격 탐지/차단 현황 요약 대상** | | | | | | | | | | | |
| **구 분** | | | **탐지건수** | | | **자동차단건수** | | | **분석 및 대응 건수** | | |
| Anti-DDoS | | | - | | | - | | | - | | |
| 웹방화벽 | | | 51,671 | | | 16,701 | | | 68,372 | | |
| IDS | | | 3,230 | | | - | | | 3,230 | | |
| IPS | | | 27,429 | | | 4,387 | | | 31,816 | | |
|  |  | |  |  | |  |  | |  |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **날짜별 공격 탐지/차단 현황** | | | | | | | |
|  | | | | | | | |
|  |  |  |  |  |  |  |  |
| **유해 IP 차단** | | | | | | | |
| **탐지장비** | | | | **건수** | | | |
| 웹방화벽 | | | | 57 | | | |
| IPS | | | | 9 | | | |
|  |  |  |  |  |  |  |  |
| **주요 이슈** | | | | | | | |
| - 특이사항 없음 | | | | | | | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **웹방화벽 공격 대응 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 특이사항요약** | | | | | | | |
| - 특이사항 없음 | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 공격 탐지/차단 현황 요약** | | | | | | | |
| **탐지 이벤트 통계** | | | | | | | |
| **구 분** | | | | **탐지건수** | | **자동차단건수** | |
| **전월 분석 및 대응 건수** | | | | 45,142 | | 17,439 | |
| **금월** | | | | 51,671 | | 16,701 | |
|  |  |  |  |  |  |  |  |
| **날짜별 공격 탐지/차단 현황** | | | | | | | |
|  | | | | | | | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 공격유형별 현황(Top 10)** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | | | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |
| **이벤트명** | | | | **탐지수** | | **차단수** | |
| Abnormal HTTP Request | | | | 51,604 | | 13,245 | |
| Command Injection | | | | 0 | | 740 | |
| Scanner/Proxy/Spambot | | | | 0 | | 668 | |
| Directory Access | | | | 0 | | 637 | |
| Application Vulnerability | | | | 0 | | 514 | |
| HTTP Method Restrictions | | | | 0 | | 455 | |
| Default Page Access | | | | 61 | | 240 | |
| URL Extension Access Control | | | | 0 | | 164 | |
| Header Vulnerability | | | | 0 | | 38 | |
| CHARSET | | | | 6 | | 0 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 공격지별 현황(Top 10)** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | | | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |
| **공격지 IP** | | | **공격지** | | | **공격/차단 건수** | |
| 149.50.103.48 | | | Poland | | | 910 | |
| 194.165.17.13 | | | Monaco | | | 93 | |
| 185.189.182.234 | | | The Netherlands | | | 47 | |
| 167.94.145.111 | | | United States | | | 16 | |
| 167.94.138.124 | | | United States | | | 7 | |
| 167.94.138.36 | | | United States | | | 6 | |
| 104.140.148.110 | | | United States | | | 1 | |
| 104.236.0.169 | | | United States | | | 1 | |
| 112.53.235.78 | | | China | | | 1 | |
| 165.154.182.92 | | | United States | | | 1 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 목적지별 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **목적지 IP** | | | **공격지 IP 수** | | | **공격/차단 건수** | |
| 112.172.179.94 | | | 25,178 | | | 53,799 | |
| 112.172.179.93 | | | 447 | | | 3,098 | |
| 112.172.179.90 | | | 375 | | | 2,346 | |
| 112.172.179.92 | | | 338 | | | 2,316 | |
| 112.172.179.91 | | | 330 | | | 2,271 | |
| 112.172.179.102 | | | 400 | | | 2,247 | |
| 112.172.179.89 | | | 317 | | | 2,231 | |
| 39.125.131.76 | | | 44 | | | 64 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **IPS 공격 대응 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 특이사항요약** | | | | | | | |
| - 특이사항 없음 | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 공격 탐지/차단 현황 요약** | | | | | | | |
| **탐지 이벤트 통계** | | | | | | | |
| **구 분** | | | | **탐지건수** | | **자동차단건수** | |
| **전월 분석 및 대응 건수** | | | | 25,432 | | 3,921 | |
| **금월** | | | | 27,429 | | 4,387 | |
|  |  |  |  |  |  |  |  |
| **날짜별 공격 탐지/차단 현황** | | | | | | | |
|  | | | | | | | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 공격유형별 현황(Top 10)** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | | | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |
| **이벤트명** | | | | **탐지수** | | **차단수** | |
| TCP PPS Limit | | | | 26,418 | | 0 | |
| Scanner Detection (User-Agent : friendly-scanner) | | | | 0 | | 2,589 | |
| RPC Portmap listing UDP 111 | | | | 0 | | 443 | |
| HTTP Sensitive URI Access Attempt(.env) | | | | 0 | | 403 | |
| Python Request Detect | | | | 291 | | 0 | |
| 1:1 TCP Flooding | | | | 132 | | 0 | |
| Web Robot Detection (User-Agent : curl) | | | | 91 | | 0 | |
| Zyxel Multiple Series CVE-2023-28771 Command Injection | | | | 77 | | 0 | |
| Scanner Detection (User-Agent : Zgrab) | | | | 0 | | 21 | |
| Ping Sweep | | | | 0 | | 12 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 공격지별 현황(Top 10)** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | | | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |
| **공격지 IP** | | | **공격지** | | | **공격/차단 건수** | |
| 173.231.184.125 | | | United States | | | 482 | |
| 185.81.30.50 | | | United States | | | 459 | |
| 112.223.74.186 | | | South Korea | | | 248 | |
| 187.33.53.204 | | | Brazil | | | 189 | |
| 87.106.62.7 | | | Germany | | | 93 | |
| 212.38.189.77 | | | United Kingdom | | | 71 | |
| 222.114.199.89 | | | South Korea | | | 64 | |
| 185.85.239.11 | | | Türkiye | | | 24 | |
| 167.94.138.150 | | | United States | | | 6 | |
| 211.245.129.120 | | | South Korea | | | 3 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 목적지별 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **목적지 IP** | | | **공격지 IP 수** | | | **공격/차단 건수** | |
| 112.172.179.92 | | | 1,233 | | | 11,079 | |
| 112.172.179.90 | | | 2,817 | | | 9,301 | |
| 112.172.179.94 | | | 3,506 | | | 4,202 | |
| 39.125.131.76 | | | 3,007 | | | 3,555 | |
| 112.172.179.91 | | | 667 | | | 1,169 | |
| 112.172.179.89 | | | 506 | | | 1,102 | |
| 112.172.179.93 | | | 345 | | | 884 | |
| 112.172.179.102 | | | 128 | | | 524 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **IDS 공격 대응 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 특이사항요약** | | | | | | | |
| - 특이사항 없음 | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 공격 탐지/차단 현황 요약** | | | | | | | |
| **탐지 이벤트 통계** | | | | | | | |
| **구 분** | | | | **탐지건수** | | **자동차단건수** | |
| **전월 분석 및 대응 건수** | | | | 3,052 | | 0 | |
| **금월** | | | | 3,230 | | 0 | |
|  |  |  |  |  |  |  |  |
| **날짜별 공격 탐지/차단 현황** | | | | | | | |
|  | | | | | | | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 공격유형별 현황(Top 10)** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | | | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |
| **이벤트명** | | | | **탐지수** | | **차단수** | |
| icmp flooding | | | | 2,438 | | 0 | |
| icmp redirect host | | | | 324 | | 0 | |
| OpenSSL DTLS CVE-2014-0221 Remote Denial of Service Vulnerability 1 | | | | 255 | | 0 | |
| tcp null scan | | | | 143 | | 0 | |
| udp service scan | | | | 27 | | 0 | |
| afs client | | | | 15 | | 0 | |
| http apache server-status | | | | 15 | | 0 | |
| tcp port scan - flag syn | | | | 5 | | 0 | |
| parameter xss vulnerability | | | | 4 | | 0 | |
| GNU Bash CVE-2014-6271 Remote Code Execution Vulnerability | | | | 1 | | 0 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 공격지별 현황(Top 10)** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  | | | | | | | |
|
|
|
|
|
|
|
|
|
|
|
|
|  |  |  |  |  |  |  |  |
| **공격지 IP** | | | **공격지** | | | **공격/차단 건수** | |
| 199.45.154.181 | | | United States | | | 6 | |
| 61.243.114.162 | | | China | | | 4 | |
| 118.235.2.138 | | | South Korea | | | 4 | |
| 167.94.138.139 | | | United States | | | 3 | |
| 106.101.67.78 | | | South Korea | | | 3 | |
| 106.101.192.245 | | | South Korea | | | 2 | |
| 106.101.197.56 | | | South Korea | | | 2 | |
| 106.102.142.42 | | | South Korea | | | 2 | |
| 106.101.67.188 | | | South Korea | | | 1 | |
| 118.235.66.79 | | | South Korea | | | 1 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **■ 목적지별 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **목적지 IP** | | | **공격지 IP 수** | | | **공격/차단 건수** | |
| 39.125.131.76 | | | 619 | | | 1,122 | |
| 112.172.179.94 | | | 591 | | | 826 | |
| 112.172.179.91 | | | 377 | | | 499 | |
| 112.172.179.89 | | | 118 | | | 301 | |
| 112.172.179.92 | | | 119 | | | 281 | |
| 112.172.179.93 | | | 56 | | | 76 | |
| 112.172.179.90 | | | 45 | | | 67 | |
| 112.172.179.102 | | | 42 | | | 58 | |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **유해 IP 차단 현황** | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 특이사항 요약** | | | | | | | |
| - 특이사항 없음 | | | | | | | |
|  |  |  |  |  |  |  |  |
| **■ 차단현황 요약** | | | | | | | |
| **날짜** | **공격지 IP** | | **공격지** | **차단사유** | | | |
| 2024-08-01 12:42:46 | 213.199.51.111 | | Canada | - PHPUnit 취약점을 이용한 원격 코드 실행 시도 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-02 10:11:38 | 188.166.166.125 | | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-02 11:13:38 | 64.226.67.238 | | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-02 11:18:07 | 134.122.75.39 | | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-02 11:43:43 | 47.83.0.196 | | United States | - Apache HTTP Server 경로 우회 취약점을 이용한 원격코드 실행 시도  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-03 05:24:20 | 91.92.250.40 | | Bulgaria | - AndroxGh0st 악성 공격툴을 이용한 스캐닝 확인  - 공격 IP 임시 차단 | | | |
| 2024-08-04 23:14:26 | 194.50.16.221 | | The Netherlands | - 웹서버 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-07 14:18:58 | 35.216.203.226 | | Switzerland | - Apache 서버 상태 페이지 접근 시도 확인  - 공격 IP 임시 차단 | | | |
| 2024-08-09 23:52:54 | 161.35.16.163 | | Germany | - 웹서버 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-10 11:15:16 | 134.122.94.120 | | Germany | - Go-http-client를 이용한 정보수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-10 15:04:12 | 164.90.173.182 | | Germany | - Go-http-client를 이용한 정보수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-10 23:48:01 | 67.220.74.204 | | United States | - 웹서버 정보 수집 스캐닝 확인  - 공격 IP 임시 차단 | | | |
| 2024-08-12 00:01:53 | 67.220.74.204 | | United States | - 웹서버 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 | | | |
| 2024-08-13 08:13:09 | 202.152.4.70 | | Indonesia | - PHPUnit 취약점을 이용한 원격 코드 실행 시도 확인  - 공격 IP 임시 차단 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 2024-08-14 12:12:30 | 167.172.173.175 | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-14 19:11:20 | 209.38.196.207 | Germany | - 웹서버 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-14 22:02:28 | 43.155.139.105 | South Korea | - WHOIS 조회 결과 Tencent Cloud Computing로 확인  - Apache HTTP Server 경로 우회 취약점을 이용한 원격코드 실행 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-16 11:12:18 | 84.32.41.186 | United Kingdom | - 정보수집을 위한 비정상 요청시도 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-17 08:07:13 | 13.53.146.244 | Sweden | - Git 디렉토리 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-17 18:32:38 | 172.87.31.10 | United States | - Apache Tomcat 관리자 페이지 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-18 20:57:36 | 89.190.156.137 | The Netherlands | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-18 22:07:18 | 89.190.156.137 | The Netherlands | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-19 03:56:01 | 144.217.240.177 | Canada | - PHPUnit 취약점을 이용한 원격 코드 실행 시도 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-19 17:57:00 | 176.123.1.32 | Moldova | - 취약 페이지 접근 시도 확인  - IP 평판조회시 악성행위 이력 확인  - 공격 IP 임시 차단 |
| 2024-08-21 11:17:17 | 159.89.111.223 | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-21 12:44:43 | 165.227.150.253 | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-21 16:44:29 | 87.239.29.132 | Russia | - PHPUnit 취약점을 이용한 원격 코드 실행 시도 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-22 16:32:43 | 206.189.38.150 | Singapore | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-22 18:40:56 | 206.189.38.150 | Singapore | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-23 22:02:25 | 78.153.140.151 | United Kingdom | - 취약 페이지 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-25 01:08:48 | 35.216.218.233 | Switzerland | - 서버 상태 확인 페이지 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-25 02:52:17 | 150.138.77.160 | China | - python-requests/2.29.0 를 이용한 phpmyadmin 페이지 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-25 16:58:30 | 79.124.59.226 | Bulgaria | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-25 17:42:29 | 79.124.59.226 | Bulgaria | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-25 18:01:33 | 79.124.59.226 | Bulgaria | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-25 18:12:08 | 79.124.59.226 | Bulgaria | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-25 18:23:27 | 79.124.59.226 | Bulgaria | - Masscan tool을 이용한 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-27 10:19:43 | 134.209.69.219 | United States | - ThinkPHP 취약점을 이용한 원격 코드 실행 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-27 11:24:39 | 46.101.160.163 | Germany | - Go-http-client 를 이용한 정보 수집 스캐닝 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |
| 2024-08-29 18:08:43 | 212.50.247.207 | United States | - 웹 서버 정보수집 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-29 18:09:51 | 182.119.128.116 | China | - 웹서버 정보 수집 스캐닝 확인  - 공격 IP 임시 차단 |
| 2024-08-29 19:13:58 | 179.43.133.242 | Switzerland | - 취약 페이지 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-30 23:23:30 | 77.237.241.114 | Germany | - 환경설정 파일 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-31 00:08:13 | 185.82.219.179 | Bulgaria | - 취약 페이지 접근 시도 확인  - 공격 IP 임시 차단 |
| 2024-08-31 19:34:33 | 213.199.53.204 | Canada | - PHPUnit 취약점을 이용한 원격 코드 실행 시도 확인  - 금보원 제공 유해 IP  - 공격 IP 임시 차단 |

|  |
| --- |
|  |

**Anti-Virus 보호 대상 서버**

|  |  |  |  |
| --- | --- | --- | --- |
| **번호** | **서버명** | **IP** | **등록일시** |
| 1 | hli-fmw-prd-srv-web-1(19092318) | 10.239.9.11 | 2023-11-09 19:08:03.0 |
| 2 | hli-fmw-prd-srv-was-1(19039609) | 10.239.10.11 | 2023-11-09 19:08:03.0 |
| 3 | hli-fmw-prd-srv-web-2(19092343) | 10.239.9.12 | 2023-11-09 19:08:03.0 |
| 4 | hli-fmw-prd-srv-was-2(19039651) | 10.239.10.12 | 2023-11-09 19:08:03.0 |
| 5 | hli-nxl-prd-srv-mng-2(20545063) | 10.239.19.121 | 2023-11-21 17:15:51.0 |
| 6 | hli-nxl-prd-srv-mng-1(20329449) | 10.239.19.120 | 2023-11-21 17:15:51.0 |
| 7 | hli-nxl-prd-knp-ifr1-w-1um0(20326181) | 10.239.22.10 | 2023-11-21 17:15:51.0 |
| 8 | hli-nxl-prd-knp-ifr1-w-1ulz(20326178) | 10.239.22.9 | 2023-11-21 17:15:51.0 |
| 9 | hli-nxl-prd-knp-sol1-w-1ulu(20326115) | 10.239.21.11 | 2023-11-21 17:15:51.0 |
| 10 | hli-nxl-prd-knp-sol1-w-1ult(20326111) | 10.239.21.10 | 2023-11-21 17:15:51.0 |
| 11 | hli-nxl-prd-knp-sol1-w-1uls(20326107) | 10.239.21.9 | 2023-11-21 17:15:51.0 |
| 12 | hli-nxl-prd-knp-nlm1-w-1uk6(20316970) | 10.239.19.11 | 2023-11-21 17:15:51.0 |
| 13 | hli-nxl-prd-knp-nlm1-w-1uk5(20316967) | 10.239.19.10 | 2023-11-21 17:15:51.0 |
| 14 | hli-nxl-prd-knp-nlm1-w-1uk4(20316963) | 10.239.19.9 | 2023-11-21 17:15:51.0 |
| 15 | hli-nxl-prd-knp-grt1-w-1uk0(20316905) | 10.239.17.11 | 2023-11-21 17:15:51.0 |
| 16 | hli-nxl-prd-knp-grt1-w-1ujz(20316902) | 10.239.17.10 | 2023-11-21 17:15:51.0 |
| 17 | hli-nxl-prd-knp-grt1-w-1ujy(20316899) | 10.239.17.9 | 2023-11-21 17:15:51.0 |
| 18 | hli-nxl-prd-knp-gaa1-w-1uju(20316723) | 10.239.15.11 | 2023-11-21 17:15:51.0 |
| 19 | hli-nxl-prd-knp-gaa1-w-1ujt(20316720) | 10.239.15.10 | 2023-11-21 17:15:51.0 |
| 20 | hli-nxl-prd-knp-gaa1-w-1ujs(20316717) | 10.239.15.9 | 2023-11-21 17:15:51.0 |
| 21 | hli-lpf-prd-nks-node-w-1tgh(20048242) | 10.239.5.11 | 2023-11-21 17:15:51.0 |
| 22 | hli-lpf-prd-nks-node-w-1tgg(20048239) | 10.239.5.10 | 2023-11-21 17:15:51.0 |
| 23 | hli-lpf-prd-nks-node-w-1tgf(20048236) | 10.239.5.9 | 2023-11-21 17:15:51.0 |
| 24 | hli-nxl-prd-knp-gaa1-w-1zra(22228771) | 10.239.15.12 | 2024-02-06 21:00:27.0 |

|  |
| --- |
| **Anti-Virus 탐지 현황 요약** |
| |  |  | | --- | --- | |  | **탐지건수** | | Anti-Virus | 1 | |

|  |  |
| --- | --- |
| **주요 이슈** | |
| * 특이사항 없습니다. | |
| **Anti-Virus 대응 현황** |

**□ 특이사항 요약**

|  |
| --- |
| 1건의 이벤트가 탐지되었으나 영향력 없는 것으로 확인되었습니다. |

**□ 공격 탐지 현황 요약**

|  |  |
| --- | --- |
| **탐지 이벤트 통계** | |
| **구분** | **탐지건수** |
| 전월 | 1 |
| 금월 | 1 |

**□ 탐지 이벤트 현황 (Top 10)**

|  |  |  |
| --- | --- | --- |
| **탐지 이벤트** | **탐지경로** | **탐지건수** |
| Mal\_Hifrm-3 | /hli\_app/sw/was/wtagent/logs/hli-nxl-prd-cos-be-6f5fdf677f-bxqsk/site/hli-nxl-prd-cos-be\_198.18.1.205\_hli-nxl-prd-cos-be-6f5fdf677f-bxqskWEB\_879C4AC74B31A8899ADAFA37B17546C0\_20240827003719.log | 1 |

**□ 탐지IP 현황 (Top 10)**

|  |  |
| --- | --- |
| **탐지IP** | **탐지건수** |
| 10.239.15.9 | 1 |