

SECURITY DAILY REPORT

MSS(Managed Security Service)



24x365



Security



AI analytics

1. 보안동향

아파치오프비즈에서 발견된 초고위험도 취약점, 공격자들은 스캔 중

[미리보기]

요약 : 보안 블로그 시큐리티어페어즈에 의하면 아파치오프비즈(Apache OFBiz)에서 초고위험도 취약점이 발견됐다고 한다. CVE-2024-38856 이며, 18.12.14 까지에 이르는 버전들에서 발견되며, 18.12.15 에서 해결됐다. 공격자들은 이미 해킹 공격을 실시하는 중에 있기 때문에 오프비즈 사용자들이라면 하루라도 빨리 18.12.15 버전을 설

[바로가기](#)

윈도에 기본 장착된 보안 기능 두 개, 설계 결함 가지고 있다

[미리보기]

요약 : 보안 외신 해커뉴스에 의하면 마이크로소프트의 윈도우 스마트 앱 컨트롤(Windows Smart App Control)과 스마트스크린(SmartScreen) 기능에서 설계 취약점이 발견됐다고 한다. 이 취약점을 익스플로잇 할 경우 원하는 환경에 침투할 수 있게 되는데, 이 때 아무런 경보도 울리지 않는다고 한다. 둘 다 윈도우에 기본 장착되어 있는 보안

[바로가기](#)

IT 전문가들만 노리는 랜섬웨어 공격자들, 새 멀웨어까지 동원해

[미리보기]

요약: 보안 외신 블리핑컴퓨터에 의하면 IT 개발자들을 노리는 랜섬웨어 캠페인이 발견됐다고 한다. 이들이 공격에 사용하는 건 새로운 유형의 '원격 접근 트로이목마(RAT)'인 샤프라이노(SharpRhino)라고 한다. 이를 통해 개발자들의 개발 환경에 침투한 후 여러 단계에 걸쳐 권한을 높이고 더 많은 부분에 침투한 뒤 랜섬웨어 페이로드를 마지막에 심는다

[바로가기](#)

LG 유플러스, '유플러스닷컴'과 '당신의 U+' 정보보호 국제인증 획득

[미리보기]

ISO 27001, ISO 27701, ISO 27017, ISO 27018 등 총 4 종자사 디지털 채널 정보보호 강화, 고객 신뢰도 높이며 안전한 서비스 제공 노력현장 실사 통해 개인정보보호 현황과 클라우드 컴퓨팅 환경 관리·운영 절차 점검[보안뉴스 김영명 기자] LG 유플러스(대표 황현식)는 자사 홈페이지 '유플러스닷컴'과 모바일 애플리케이션 '당신의 U

[바로가기](#)

제 2 의 클라우드스트라이크 사태 막아야... 시놀로지, 조직 데이터 회복력 키우는 5 가지 포인트 제시

[미리보기]

데이터 회복력의 핵심은 안전한 백업과 재해 복구 계획 갖추기포괄적인 백업, 정기적인 복구 훈련, VM 복구, 크로스 플랫폼 복구, 오프사이드 백업 및 복구 [보안뉴스 박은주 기자] 지난 7 월 클라우드스트라이크는 실시간 위협 감지 및 엔드포인트 보호를 위한 '팔콘 센서(Falcon Sensor)'를 업데이트하려다 시스템 충돌이 발생했다. 850 만 대의 마이크

[바로가기](#)

2. 보안권고문

Apache OFBiz 제품 보안 업데이트 권고

[미리보기]

Apache OFBiz 제품 보안 업데이트 권고 2024.08.06 □ 개요 ○ Apache 소프트웨어 재단은 자사 제품에서 발생하는 취약점에 대한 보안 업데이트 발표 [1] ○ ..

[바로가기](#)

Rockwell Automation 제품 보안 업데이트 권고

[미리보기]

Rockwell Automation 제품 보안 업데이트 권고 2024.08.06 □ 개요 ○ Rockwell Automation 社の 제품에서 발생하는 취약점을 해결한 보안 업데이트..

[바로가기](#)

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-08-05)

[미리보기]

2024-08-26 Apply mitigations per vendor instructions or discontinue use of the product if mitigation..

[바로가기](#)



주소 | 서울특별시 서초구 서초대로 255 고덕빌딩 2 층(06595)

전화 | 02-2105-4400 (영업문의-1 번, 보안관제문의-2 번, 기술문의-3 번)

팩스 | 02-2105-4456

영업문의 | sales@eosec.co.kr 보안관제 및 기술 문의 | tech@eosec.co.kr

©EYEON SECURITY All Right Reserved.