

SECURITY DAILY REPORT

MSS(Managed Security Service)



24x365



Security



AI analytics

1. 보안동향

티머니 전산센터 시스템 27 일 오후 한때 장애... 현재 복구 완료

[미리보기]

택시승인 서비스, 고속·시외버스 예매·발권 서비스 오류...1 시간 35 분 만에 복구[보안뉴스 김영명 기자] 27 일 오후 티머니에서 전산센터 시스템 장애가 발생해 한때 티머니 택시승인 서비스, 고속·시외버스의 예매 및 발권 서비스에 오류가 발생했던 것으로 알려졌다.티머니는 동명의 회사가 발행하는 충전식 전국 호환 교통카드다. 교통카드 시스템이 활성화되지 않은

[바로가기](#)

해킹그룹 어웨이크리코, '메시에이전트'라는 합법 툴로 러시아 공격 감행

[미리보기]

피싱 이메일에 악성 URL 삽입 배포...Go 언어로 개발된 GoLang 드로퍼 사용해 전파 총 77 개 이상의 국가에서 메시에이전트 서버 발견...독일, 미국, 프랑스 순으로 많아[보안뉴스 김영명 기자] '어웨이크리코(Awaken Likho)'라는 APT 해킹그룹이 올해 6 월부터 8 월까지 러시아 정부기관과 산업체를 주요 표적으로 삼아 새로운 공격 캠페인을

[바로가기](#)

‘건강검진 사칭’ 문자 주의보! 공식 문자에는 인터넷 주소 포함 안 돼

[미리보기]

악성코드 포함된 링크 클릭 시 휴대폰 감염시켜 개인정보 유출 피해 발생국민건강보험공단, 국가건강검진 대상자 등으로 둔갑해 개인·금융정보 탈취 사례 안내[보안뉴스 김영명 기자] 국민건강보험공단(이사장 정기석)은 최근 건강검진 수검자가 집중되는 연말에 공단을 사칭하는 사기문자가 국민에게 발송될 수 있다며 각별한 주의를 당부했다.건강검진 문자 사기는 ‘국민건강보

[바로가기](#)

개인정보위, ‘제 46 차 GPA’에서 인공지능 시대 개인정보 이슈 논의 주도

[미리보기]

10 월 28 일~11 월 1 일, 영국령 저지에서 글로벌 프라이버시 총회 열려인공지능 시대 안전한 국경 간 데이터 이전 등 개인정보 정책 과제 논의유럽연합, 영국, 프랑스, 싱가포르 등 개인정보 감독기구와 양자 회의...상호 협력 강조[보안뉴스 김영명 기자] 개인정보보호위원회(이하 개인정보위) 고학수 위원장이 10 월 28 일부터 11 월 1 일까지 영국령 저지(Bai

[바로가기](#)

파인더갭 버그바운티 플랫폼, ‘2024 우수 정보보호 기술 지정’ 성과

[미리보기]

과기정통부와 KISA 공동 주관...정보보호 분야 유망 신기술, 성장 지원 목적으로 운영윤리적 해커에 대한 KYC 인증 절차 및 VDI 나 VPN 통한 접근만 허용해 서비스 보안 강화[보안뉴스 김영명 기자] 정보보안 전문 스타트업 파인더갭(대표 김오중)의 ‘파인더갭 버그바운티 플랫폼’이 과학기술정보통신부와 한국인터넷진흥원(KISA)이 주관하는 ‘2024 우수

[바로가기](#)

2. 보안권고문

Grafana Labs 제품 보안 업데이트 권고

[미리보기]

Grafana Labs 제품 보안 업데이트 권고 2024.10.25 개요 o Grafana Labs社は 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표[1] o 영향받는 버전을 사용 중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 o 설명 o Grafana에서 발생하는 원격 코드 실행 가능한 Command Injection 및 LFI 취약점(CVE-2024-9264) [1][2] o 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-9264 Grafana 11.0.x 11.0.5+security-01 11.0.6+security-01 11.1.x 11.1.6+security-01 11.1.7+security-01 11.2.x 11.2.1+security-01 11.2.2+security-01 ※하단의 참고사이트를 확인하여 업데이트 수행[1][3] o 참고사이트 [1]<https://grafana.com/blog/2024/10/17/grafana-security-release-critical-severity-fix-for-cve-2024-9264/> [2]<https://nvd.nist.gov/vuln/detail/CVE-2024-9264> [3]<https://grafana.com/security/security-advisories/cve-2024-9264/> o 문의사항 o 한국인터넷진흥원 사이버민원센터:국번없이 118 o 작성:위협분석단 취약점분석팀 키워드 Grafana Labs, Grafana

바로가기

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-10-24)

[미리보기]

2024-11-14 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) contain a missing release of resource after effective lifetime vulnerability that could allow an unauthenticated, remote attacker to cause a denial-of-service (DoS) of the RAVPN service. 2024-10-24 Cisco ASA and FTD Denial-of-Service Vulnerability Cisco CVE-2024-20481 2024-11-14 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. RoundCube Webmail contains a cross-site scripting (XSS) vulnerability in the handling of SVG animate attributes that allows a remote attacker to run malicious JavaScript code. 2024-10-24 RoundCube Webmail Cross-Site Scripting (XSS) Vulnerability Roundcube CVE-2024-37383

바로가기



주소 | 서울특별시 서초구 서초대로 255 고덕빌딩 2층(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.