1. 보안동향

'유명'과 '무료'의 역습 : 젠데스크 피싱 주의보

[미리보기]

유명 기업용 솔루션 중 하나인 젠데스크가 교묘한 피싱 도구가 됐다. 유명한데다가 무료 서브도메인을 설정할 수 있게까지 해줘서 공격자들 사이에서 각광 받고 있다.3 줄 요약 1. 고객 관리 솔루션 젠데스크, 피싱 도구로도 활용됨.2. 무료 서브도메인 만든 후 가짜 티켓 발송한다고 속임.3. 우리 회사(혹은 잘 아는 회사)에서 보낸 티켓, 함부로 열면 안 됨.[보

바로가기

중앙대 융합보안대학원, 창립 10 주년 기념행사 열려

[미리보기]

산업보안 세미나와 기념식 융합한 10 주년 행사"4 차 산업혁명 시대에 걸맞은 보안 교육과 연구 진행"[보안뉴스 조재호 기자] 중앙대학교 융합보안학과 대학원 창립 10 주년 기념식이 중앙대 서울 캠퍼스에서 23 일 열렸다. 행사에는 대학원 교수와 재학생을 비롯해 졸업생과 보안산업 관계자 80 여 명이 참석했다. 노승민 대학원 학과장을 대신해 연단에 선 신동천 교수는

바로가기

카스퍼스키, 북한발 新악성코드 발견

[미리보기]

3 줄 요약북한 연계 해킹조직 '라자루스'의 백도어 발견주로 핵 연구소나 방위산업체 위주로 사이버 공격"고급 솔루션과 글로벌 협력의 중요성 재확인한 계기"[보안뉴스 조재호 기자] 핵 시설 근무자 대상 북한의 사이버 공격이 감지됐다. 카스퍼스키 글로벌 연구 분석팀(GReAT)은 최근 북한과 연계된 해킹 조직 라자루스(Lazarus)가 새로운 모듈식 백도어 'C

바로가기

[부고] 조용만 비즈워치 이사회의장 모친상

[미리보기]

△ 내용 : 조용만 비즈워치 이사회의장 모친상△ 고인 : 故 오무금 님 (87 세)△ 발인 : 1 월 25 일(토) 오전 9 시 00 분△ 빈소 : 창원경상대병원 장례식장 특 1 호실△ 장지 : 창원공원묘원[조재호 기자(sw@boannews.com)]<저작권자: 보안뉴스(www.boannews.com) 무단전재-재배포금지>

바로가기

국정원, 국가망보안체계 보안대책 제시...N²SF 가이드라인 발표

[미리보기]

3 줄요약 1. 국정원, 공공데이터 활용 촉진·보안성 확보 위한 국가망보안체계 보안대책 제시 2. 기밀(C)·민감(S)·공개(O) 등급에 따라 보안대책 차등 적용 3. 6 개 보안통제 항목 적용해야[보안뉴스 김경애 기자] 국정원 국가망보안체계 보안대책이 베일을 벗었다. 보안대책은 총 6 개 보안통제 항목으로 ①권한 ②인증 ③분리 및 격리 ④통제 ⑤데이터 ⑥정보자산

바로가기

---

2. 보안권고문

Cisco 제품 보안 업데이트 권고

[미리보기]

Cisco 제품 보안 업데이트 권고 2025.01.23 ㅁ 개요 o Cisco 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1][2][3] o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o Cisco BroadWorks 의 SIP 에서 발생하는 서비스 거부 취약점(CVE-2025-20165) [1][4] o Cisco Meeting Management 의 REST API 에서 발생하는 권한 상승 취약점(CVE-2025-20156) [2][5] o Cisco Unified Industrial Wireless 소프트웨어의 웹 기반 관리 인터페이스에서 발생하는 Command Injection 취약점(CVE-2025-20418) [3][6] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2025-20165 Cisco BroadWorks RI.2024.11 미만 RI.2024.11 CVE-2025-20156 Cisco Meeting Management 3.8 이하 고정된 릴리스로 마이그레이션 (3.9.1, 3.10) 3.9 3.9.1 CVE-2024-20418 Cisco Unified Industrial Wireless 17.14 이하 고정된 릴리스로 마이그레이션 (17.15.1) 17.15 17.15.1 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1][2][3][7] ㅁ 참고사이트 [1]
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-sip-dos-mSySbrmt [2]
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc [3]
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs [4]
https://nvd.nist.gov/vuln/detail/CVE-2025-20165 [5] https://nvd.nist.gov/vuln/detail/CVE-2025-20156 [6]
https://nvd.nist.gov/vuln/detail/CVE-2024-20418 [7] https://www.cisco.com/c/en/us/support/index.html ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성: 위협분석단 취약점분석팀 키워드 Cisco BroadWorks , Cisco Meeting Management , Cisco Unified Industrial Wireless

바로가기

Eyeon Security
information security company

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