1. 보안동향

최근 4 년간 교육기관 개인정보 유출, 615 만건 넘었다... 올해도 8 월까지 52 만여건

[미리보기]

2021 년 4 만여건, 2022 년에는 전년 대비 37.7 배 급증...개인정보 유출 꾸준한 증가세 보여최근 3 년간 개인정보 유출사고 2 배 증가, 유출규모는 98 배 이상 증가진선미 의원, "개인정보 보호보다 개인정보 활용에 초점 둔 현 정부의 교육정책이 그 원인"[보안뉴스 김영명 기자] 교육청과 일선학교, 대학과 대학병원 등 교육기관들에서 개인정보 유출사고와 규

바로가기

[오늘의 보안 영어] let alone

[미리보기]

"It is unusual for China's central bank to ease on two fronts at once, let alone three. Pan Gongsheng, the PBoC's governor, said it might do more in the near future, perhaps cutting reserve requiremen

바로가기

인터넷아카이브 해킹 사건으로 3100 만 명의 정보 유출돼

[미리보기]

요약 : 보안 외신 블리핑컴퓨터에 의하면 인터넷아카이브(Internet Archive)가 해킹 당했다고 한다. 한 해커가 인터넷아카이브의 TheWayback Machine 웹사이트를 해킹했으며, 이를 통해 사용자들의 인증 관련 데이터베이스를 훔쳐가는 데 성공한 것으로 보인다. 약 3100 만 명의 사용자들이 영향을 받은 것으로 알려져 있다. 해커 스스로가

바로가기

러시아 정부 집중적으로 노리는 어웨이큰리코, 아직 활동 중

[미리보기]

요약 : 러시아 정부 기관을 집중적으로 공격하는 사이버 공격 단체가 나타났다. 보안 업체 카스퍼스키(Kaspersky)를 인용한 보안 외신 시큐리티어페어즈에 의하면 어웨이큰리코(Awaken Likho)라고 하며, 지난 6 월부터 8 월까지 러시아를 겨냥한 캠페인을 활발히 실시했다고 한다. 주로 피싱 공격을 통해 멀웨어를 퍼트리려는 목적으로 진행됐으며, 이 멀웨

바로가기

주력 산업 현장에서 사용되는 MMS 에서 다섯 가지 취약점 발견돼

[미리보기]

요약 : 보안 외신 해커뉴스에 의하면 산업 현장에서 주력으로 사용되고 있는 MMS 프로토콜 생태계에서 다량의 취약점이 발견됐다고 한다. 이 취약점들을 익스플로잇 하는 데 성공할 경우 산업 현장에 생산 중단, 물리적 손상 등 여러 가지 영향을 미칠 수 있게 된다. 문제가 되고 있는 라이브러리는 MZ 오토메이션(MZ Automation)의 libIEC61850

바로가기

---

2. 보안권고문

Palo Alto Networks 제품 보안 업데이트 권고

[미리보기]

Palo Alto Networks 제품 보안 업데이트 권고 2024.10.10 □ 개요 o Palo Alto Networks 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 □ 설명 o Palo Alto Networks 의 Expedition 에서 발생하는 OS Command Injection 취약점 (CVE-2024-9463) [1][2] o Palo Alto Networks 의 Expedition 에서 발생하는 OS Command Injection 취약점 (CVE-2024-9464) [1][3] o Palo Alto Networks 의 Expedition 에서 발생하는 SQL Injection 취약점 (CVE-2024-9465) [1][4] o Palo Alto Networks 의 Expedition 에서 발생하는 민감 정보 노출 취약점 (CVE-2024-9466) [1][5] o Palo Alto Networks 의 Expedition 에서 발생하는 Reflected XSS 취약점 (CVE-2024-9467) [1][6] □ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-9463 CVE-2024-9464 CVE-2024-9465 CVE-2024-9466 CVE-2024-9467 Expedition 1.2.96 미만 1.2.96 이상 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1][7] □참고사이트 [1] https://security.paloaltonetworks.com/PAN-SA-2024-0010 [2] https://nvd.nist.gov/vuln/detail/CVE-2024-9463 [3] https://nvd.nist.gov/vuln/detail/CVE-2024-9464 [4] https://nvd.nist.gov/vuln/detail/CVE-2024-9465 [5] https://nvd.nist.gov/vuln/detail/CVE-2024-9466 [6] https://nvd.nist.gov/vuln/detail/CVE-2024-9467 [7] https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340 □ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 □ 작성:위협분석단 취약점분석팀 키워드 Palo Alto Networks, Expedition

바로가기

Mozilla 제품 보안 업데이트 권고

[미리보기]

Mozilla 제품 보안 업데이트 권고 2024.10.10 □개요 o Mozilla 재단은 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표[1] o 영향받는 버전을 사용 중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 □설명 o Firefox, Firefox ESR 에서 발생하는 Use-After-Free 취약점(CVE-2024-9680)[1][2] □영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-9680 Firefox 131.0.2 미만 131.0.2 Firefox ESR 128.3.1 미만 128.3.1 115.16.1 미만 115.16.1 ※하단의 참고사이트를 참고하여 해결된 버전으로 업데이트 수행[1][3][4][5] [참고사이트] [1] https://www.mozilla.org/en-US/security/advisories/mfsa2024-51/ [2] https://nvd.nist.gov/vuln/detail/CVE-2024-9680 [3] https://www.mozilla.org/en-US/firefox/131.0.2/releasenotes/ [4] https://www.mozilla.org/en-US/firefox/115.16.1/releasenotes/ [5] https://www.mozilla.org/en-US/firefox/128.3.1/system-requirements/ □ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 □ 작성:위협분석단 취약점분석팀 키워드 Mozilla , Firefox , Firefox ESR

바로가기

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-10-09)

[미리보기]

2024-10-30 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Fortinet FortiOS, FortiPAM, FortiProxy, and FortiWeb contain a format string vulnerability that allows a remote, unauthenticated attacker to execute

arbitrary code or commands via specially crafted requests. 2024-10-09 Fortinet Multiple Products Format String Vulnerability Fortinet CVE-2024-23113 2024-10-30 As Ivanti CSA 4.6.x has reached End-of-Life status, users are urged to remove CSA 4.6.x from service or upgrade to the 5.0.x line, or later, of supported solution. Ivanti Cloud Services Appliance (CSA) contains a SQL injection vulnerability in the admin web console in versions prior to 5.0.2, which can allow a remote attacker authenticated as administrator to run arbitrary SQL statements. 2024-10-09 Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability Ivanti CVE-2024-9379 2024-10-30 As Ivanti CSA 4.6.x has reached End-of-Life status, users are urged to remove CSA 4.6.x from service or upgrade to the 5.0.x line, or later, of supported solution. Ivanti Cloud Services Appliance (CSA) contains an OS command injection vulnerability in the administrative console which can allow an authenticated attacker with application admin privileges to pass commands to the underlying OS. 2024-10-09 Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability Ivanti CVE-2024-9380

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