
# 1. 보안동향

## 미국과 영국이 합동으로 내놓은 보안 경고문, “모두가 방어해야 하는 러시아 해커들”

**[미리보기]**

미국과 영국의 정보 기관들이 합동으로 러시아 해커들에 대한 경고문을 발표했다. 러시아 해커들이라고 해서 덩치가 크고 중요한 조직만 노리는 게 아니라고 이들은 강조해서 경고했다. 모두가 보안 강화에 참여해야 하기에 보안 담당자들이 잘 이해하는 언어를 적극 활용하기도 했다.[보안뉴스 문정후 기자] 미국 연방수사국(FBI)와 국가안보국(NSA), 사이버 국가임무

바로가기

---

## 인기 프랜차이즈 포켓몬으로 게임 만드는 개발사, 대규모 해킹 사고에 연루돼

**[미리보기]**

지난 8 월에 한 게임 개발사에서 해킹 사고가 발생했다. 당시 개인정보만 새나간 것으로 파악됐는데, 갑자기 주말부터 엉뚱한 정보들이 퍼지기 시작했다. 사건의 전말이 궁금해지는 상황이다.[보안뉴스 문가용 기자] 인기 프랜차이즈인 포켓몬을 가지고 게임을 제작하는 회사 게임프리크(Game Freak)에서 대규모 해킹 사고가 발생했다. 이 규모가 얼마나 큰지 게임

바로가기

---

## 앵그리 스틸러 정보탈취 악성코드, 텔레그램에서 절찬리에 판매 중

**[미리보기]**

같은 이름 텔레그램 채널에서 150 달러에 판매...수집 가능 항목, 탈취물, 제작자 프로필 게시웹브라우저·프로그램·파일·암호화폐 지갑·시스템 등 정보수집, 스크린샷 촬영 등의 불법 행위[보안뉴스 김영명 기자] 최근 텔레그램에서 판매 중인 정보탈취 악성코드 '앵그리 스틸러(Angry Stealer)'가 발견됐다. 이 악성코드는 'ANGRY STEALER'라는

바로가기

---

## [정보세계정치학회 칼럼] 공공기관 클라우드 보안기준의 필요성

**[미리보기]**

미국, 한국 클라우드 보안기준 인증인 CSAP 에 과도한 차별인 무역장벽 주장하지만 미국도 CLOUD Act 제정 등 통해 데이터 안보 관련 '공공의 안전' 제도 수립한국 역시 데이터 안보 조치로 국가 안보 관련 공공데이터 안전 보장 등 대응 필요[보안뉴스= 이효영 국립외교원 부교수] 데이터 현지화(Data Localisation) 조치는 대표적인 데이터 안

바로가기

---

## 상주·문경시청-정보통신행정연구원, 개인정보보호 실무 협의회 개최

**[미리보기]**

'개인정보보호 실무 협의회' 구성 통한 개인정보보호 대응능력 강화 모색 [보안뉴스 김경애 기자] 경북의 기초지자체인 상주시청은 문경시청과 개인정보 컨설팅 전문기업인 정보통신행정연구원과 공동으로 10 월 8 일 시청 영상회의실에서 '개인정보보호 실무 협의회'를 개최했다고 밝혔다.개인정보 유출사고는 증가하는 반면 개인정보 관계 법령은 갈수록 강화되고 있다. 202

바로가기

---

# 2. 보안권고문

## MS 10 월 보안 위협에 따른 정기 보안 업데이트 권고

**[미리보기]**

MS 10 월 보안 위협에 따른 정기 보안 업데이트 권고 2024.10.14 ㅁ10 월 보안업데이트 개요 (총 11 종) o 등급 :긴급 (Critical) 7 종 ,중요 (Important) 4 종 o 발표일 : 2024.10.08.(화) o 업데이트 내용 제품군 중요도 영향 Windows 11 v24H2, Windows 11 23H2, Windows 11 v22H2, Windows 11 v21H2 긴급 원격 코드 실행 Windows 10 22H2, Windows 10 21H2 긴급 원격 코드 실행 Windows Server 2022 23H2 버전(Server Core 설치), Windows Server 2022, Windows Server 2022(Server Core 설치) 긴급 원격 코드 실행 Windows Server 2019 긴급 원격 코드 실행 Windows Server 2016 긴급 원격 코드 실행 Microsoft Office 중요 원격 코드 실행 Microsoft SharePoint 중요 권한 상승

바로가기

---

## Veeam 제품 보안 업데이트

**[미리보기]**

Veeam 제품 보안 업데이트 2024.10.14 ㅁ 개요 o Veeam 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 ㅁ 설명 o Veeam Backup & Replication 에서 발생하는 원격 코드 실행(RCE) 취약점(CVE-2024-40711)[1][2] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-40711 Veeam Backup & Replication 12.1.2.172 이하 12.2.0.334 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [3] ㅁ 참고사이트 [1] https://www.veeam.com/kb4649 [2] https://nvd.nist.gov/vuln/detail/CVE-2024-40711 [3] https://www.veeam.com/products/downloads/latest-version.html ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성: 위협분석단 취약점분석팀 키워드 Veeam Backup & Replication

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