1. 보안동향

[긴급] 레디스 DB 시스템에서 원격 코드 실행 취약점 발견... 소규모 기업 주의

[미리보기]

레디스의 루아 엔진에서 스택 버퍼 오버플로우 오류로 원격 코드 실행 취약점 발생 악의적 코드 실행·데이터 탈취 및 서버 제어 위험...주고객인 소규모 기업은 신속한 업데이트 필요[보안뉴스 박은주 기자] 오픈소스 기반의 비관계형 데이터베이스 관리 시스템 'Redis(레디스)'에서 원격 코드 실행 취약점(RCE)이 발견됐다. 악의적 코드 실행, 데이터 탈취

바로가기

과기정통부, 제 1 회 자율주행 인공지능 챌린지 시상식 개최

[미리보기]

차량용 3D 객체 검출 분야 TakeOut(김준영)팀, 장관상 수상[보안뉴스 김영명 기자] 과학기술정보통신부(장관 유상임, 이하 과기정통부)는 11 월 19 일 대전 한국전자통신연구원(ETRI)에서 '제 1 회 자율주행 인공지능 챌린지'(이하 대회) 시상식을 개최했다고 밝혔다.이번 대회는 과기정통부가 2021 년부터 추진한 '자율주행 기술개발 혁신사업'의 연구개발

바로가기

경찰청, 딥페이크 등 디지털 성범죄 대응 위한 '글로벌 정책 대화' 개최

[미리보기]

유엔개발계획과 공동 주관...2022 년부터 경찰 역량 강화 교육 위한 1 차 시범사업 진행중디지털 성범죄 대응 경험과 지식 공유, 법률적·정책적 대응방안 분석 및 논의 예정[보안뉴스 김영명 기자] 경찰청(청장 조지호)은 유엔개발계획(United Nations Development Programme, UNDP)과 공동 주관으로 11 월 19 일부터 20 일까지 이틀

바로가기

경찰청, 19 개 국가·국제기구 참여 '제 2 회 사기방지 국제 콘퍼런스' 개최

[미리보기]

11 월 18 일~19 일, 16 개국 정부·학계, UNODC 등 3 개 국제기구, 금융·통신·플랫폼 기업 참여초 국경 조직 사기 생태계 척결 위한 민·관·학 협업, '세계는 하나의 팀' 노력'핀테크', '금융', '글로벌 온라인 플랫폼' 등 7 개 분야, 분과별 사기방지 대책 발표 및 논의[보안뉴스 김영명 기자] 경찰청(청장 조지호)은 국제적인 사기범죄 위협에 대응

바로가기

이스트시큐리티, 캐릭터 IP 신규사업 '이스트로바' 본격 시동

[미리보기]

알약이와 친구들이 판타지 모험을 통해 벌어지는 이야기를 담은 캐릭터 IP 브랜드 '이스트로바(ESTROVA)' 발표무신사, 29CM, 자사몰 등에서 디지털 액세서리·리빙·의류·잡화 카테고리로 판매 중[보안뉴스 박은주 기자] 보안전문기업 이스트시큐리티(대표 정진일)은 자체 캐릭터 IP 브랜드인 '이스트로바(ESTROVA)'를 통해 캐릭터 사업에 본격 진출했다

바로가기

---

2. 보안권고문

BROADCOM 제품 보안 업데이트 권고

[미리보기]

BROADCOM 제품 보안 업데이트 권고 2024.11.19 □ 개요 o Broadcom 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 □ 설명 o VMware vCenter Server 에서 힙 오버플로우 취약점(CVE-2024-38812) [1][2] o VMware vCenter Server 에서 발생하는 권한상승 취약점(CVE-2024-38813) [1][3] □ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-9486 VMware vCenter Server 8.0 8.0 U3d 8.0 8.0 U2e 7.0 7.0 U3t VMware Cloud Foundation 5.x 8.0 U3d (비동기 패치) 5.1.x 8.0 U2e (비동기 패치) 4.x 7.0 U3t (비동기 패치) ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1] □ 참고사이트 [1] https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968 [2] https://nvd.nist.gov/vuln/detail/CVE-2024-38812 [3] https://nvd.nist.gov/vuln/detail/CVE-2024-38813 □ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 □ 작성: 위협분석단 취약점분석팀 키워드 VMware vCenter Server , VMware Cloud Foundation

바로가기

PostgreSQL 제품 보안 업데이트 권고

[미리보기]

PostgreSQL 제품 보안 업데이트 권고 2024.11.19 □ 개요 o PostgreSQL 재단은 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 □ 설명 o PostgreSQL PL/Perl 에서 발생하는 임의 코드 실행 취약점(CVE-2024-10979) [1][2] □ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-10979 PostgreSQL PL/Perl 17.1 미만 17.1 16.5 미만 16.5 15.9 미만 15.9 14.14 미만 14.14 13.17 미만 13.17 12.21 미만 12.21 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1] □ 참고사이트 [1] https://www.postgresql.org/support/security/CVE-2024-10979/ [2] https://nvd.nist.gov/vuln/detail/CVE-2024-10979 □ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 □ 작성: 위협분석단 취약점분석팀 키워드 PostgreSQL PL/Perl

바로가기

시큐위즈 VPN 제품 취약점 보안 업데이트 권고

[미리보기]

시큐위즈 VPN 제품 취약점 보안 업데이트 권고 2024.11.19 □ 개요 o 시큐위즈社의 Secuway SSL VPN 제품에서 발생하는 취약점 발견 o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 보안 조치 필요 □ 설명 o 애플 기기를 통한 민감 데이터의 불충분한 보호 취약점 (CWE-922) o 애플 기기를 통한 시스템 인증 우회 취약점 (CWE-287) □ 영향받는 제품 및 해결 방안 제품명 영향받는 버전 해결 방안 Secuway SSL VPN U1.0 제조사로부터 전달받은 패치 파일을 적용하고 버전 정보에 "/ 패치날짜_T4" 가 추가되었는지 여부 확인 U2.0 ※ 취약점 패치 전까지 애플 기기를 이용한 VPN 로그인 차단 필요 □ 문의사항 o 시큐위즈社 연락처 : 02-6380-3680 - 홈페이지 :

https://www.secuwiz.co.kr o 침해사고 발생 시 아래 절차를 통해 침해사고 신고 ※ 보호나라(https://boho.or.kr) → 침해사고 신고 → 신고하기 ㅁ 작성: 위협분석단 취약점분석팀 키워드 시큐위즈 , Secuway SSL VPN

바로가기

Redis 제품 보안 업데이트 권고

[미리보기]

Redis 제품 보안 업데이트 권고 2024.11.19 ㅁ 개요 o Redis 社는 자사 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표 [1] o 영향받는 버전을 사용 중인 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고 ㅁ 설명 o Redis 에서 발생하는 원격 코드 실행(RCE) 취약점(CVE-2024-31449) [1][2][3] ㅁ 영향받는 제품 및 해결 방안 취약점 제품명 영향받는 버전 해결 버전 CVE-2024-31449 Redis 모든 Redis 소프트웨어 릴리스 7.4.2-169 이상, 7.2.4-109 이상, 6.4.2-110 이상, 7.4.6 – 모든 빌드, 7.6.0 – 모든 빌드(non-GA), 7.8.0 – 모든 빌드(non-GA) 모든 Redis OSS/CE/Stack 릴리스 (OSS/CE)7.4.1, (OSS/CE)7.2.6, (OSS/CE)6.2.16, (Stack)7.4.0-v1, (Stack)7.2.0-v13, (Stack)6.2.6-v17 ※ 하단의 참고사이트를 확인하여 업데이트 수행 [1] ㅁ 참고사이트 [1] https://redis.io/blog/security-advisory-cve-2024-31449-cve-2024-31227-cve-2024-31228/ [2] https://github.com/redis/redis/security/advisories/GHSA-whxg-wx83-85p5 [3] https://nvd.nist.gov/vuln/detail/CVE-2024-31449 ㅁ 문의사항 o 한국인터넷진흥원 사이버민원센터: 국번없이 118 ㅁ 작성: 위협분석단 취약점분석팀 키워드 Redis

바로가기

MS 11 월 보안 위협에 따른 정기 보안 업데이트 권고

[미리보기]

MS 11 월 보안 위협에 따른 정기 보안 업데이트 권고 2024.11.19 ㅁ11 월 보안업데이트 개요 (총 13 종) o 등급 :긴급 (Critical) 8 종 ,중요 (Important) 5 종 o 발표일 : 2024.11.12.(화) o 업데이트 내용 제품군 중요도 영향 Windows 11 v24H2, Windows 11 23H2, Windows 11 v22H2, 긴급 권한 상승 Windows 10 22H2 중요 권한 상승 Windows Server 2025, Windows Server 2025(Server Core 설치) 긴급 권한 상승 Windows Server 2022 23H2 버전(Server Core 설치), Windows Server 2022, Windows Server 2022(Server Core 설치) 긴급 권한 상승 Windows Server 2019 긴급 권한 상승 Windows Server 2016 긴급 권한 상승 Microsoft Office 중요 원격 코드 실행 Microsoft Exchange Server 중요 보안 기능 우회 Microsoft .NET 긴급 원격 코드 실행 Microsoft Visual Studio 긴급 원격 코드 실행 Microsoft SQL Server 중요 원격 코드 실행 Microsoft Azure 긴급 권한 상승 System Center 중요 원격 코드 실행 [참고 사이트] [1] (한글)https://msrc.microsoft.com/update-guide/ko-kr/ [2] (영문)https://msrc.microsoft.com/update-guide/en-us/ [3]https://msrc.microsoft.com/update-guide/ko-kr/releaseNote/2024-Nov o 취약점 요약 정보 (총 161 개) 제품 카테고리 CVE 번호 CVE 제목 Microsoft Edge (Chromium-based) CVE-2024-9966 Chromium: CVE-2024-9966 탐색에서 부적절한 구현 Microsoft Edge (Chromium-based) CVE-2024-9965 Chromium: CVE-2024-9965 DevTools 에서 불충분한 데이터 유효성 검사 Microsoft Edge (Chromium-based) CVE-2024-9964 Chromium: CVE-2024-9964 결제에서 부적절한 구현 Microsoft Edge (Chromium-based) CVE-2024-9963 Chromium: CVE-2024-9963 다운로드에서 불충분한 데이터 유효성 검사 Microsoft Edge (Chromium-based) CVE-2024-9962 Chromium: CVE-2024-9962 사용 권한에서 부적절한 구현 Microsoft Edge (Chromium-based) CVE-2024-9961 Chromium: CVE-2024-9961 Parcel Tracking 에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-9960 Chromium: CVE-2024-9960 Dawn 에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-9959 Chromium: CVE-2024-9959 DevTools 에서 UaF(Use after free) Microsoft Edge (Chromium-based)

CVE-2024-9958 Chromium: CVE-2024-9958 PictureInPicture 에서 부적절한 구현 Microsoft Edge (Chromium-based) CVE-2024-9957 Chromium: CVE-2024-9957 UI 에서 해제 후 사용 Microsoft Edge (Chromium-based) CVE-2024-9956 Chromium: CVE-2024-9956 웹 인증에서 부적절한 구현 Microsoft Edge (Chromium-based) CVE-2024-9955 Chromium: CVE-2024-9955 웹 인증에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-9954 Chromium: CVE-2024-9954 AI 에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-9603 Chromium: CVE-2024-9603 V8 에서 유형 혼란 Microsoft Edge (Chromium-based) CVE-2024-9602 Chromium: CVE-2024-9602 V8 에서 유형 혼란 Windows cURL Implementation CVE-2024-6197 Hackerone: CVE-2024-6197 utf8asn1str 에서 스택 버퍼 해제 Microsoft Defender for Endpoint CVE-2024-5535 OpenSSL: CVE-2024-5535 SSL_select_next_proto 버퍼 덮어쓰기됨 Azure Stack CVE-2024-49060 Azure Stack HCI Elevation of Privilege Vulnerability Airlift.microsoft.com CVE-2024-49056 Airlift.microsoft.com 권한 상승 취약성 Microsoft PC Manager CVE-2024-49051 Microsoft PC Manager 권한 상승 취약성 Visual Studio Code CVE-2024-49050 Visual Studio Code Python 확장 원격 코드 실행 취약성 Visual Studio Code CVE-2024-49049 Visual Studio Code 원격 확장 권한 상승 취약성 TorchGeo CVE-2024-49048 TorchGeo 원격 코드 실행 취약성 Windows Win32 Kernel Subsystem CVE-2024-49046 Windows Win32 커널 하위 시스템 권한 상승 취약성 Visual Studio CVE-2024-49044 Visual Studio 권한 상승 취약성 SQL Server CVE-2024-49043 Microsoft.SqlServer.XEvent.Configuration.dll 원격 코드 실행 취약성 Azure Database for PostgreSQL CVE-2024-49042 Azure Database for PostgreSQL 유연한 서버 확장 권한 상승 취약성 Microsoft Exchange Server CVE-2024-49040 Microsoft Exchange Server 스푸핑 취약성 Windows Task Scheduler CVE-2024-49039 Windows 작업 스케줄러 권한 상승 취약성 Microsoft Office Word CVE-2024-49033 Microsoft Word 보안 기능 우회 취약성 Microsoft Graphics Component CVE-2024-49032 Microsoft Office 그래픽 원격 코드 실행 취약성 Microsoft Graphics Component CVE-2024-49031 Microsoft Office 그래픽 원격 코드 실행 취약성 Microsoft Office Excel CVE-2024-49030 Microsoft Excel 원격 코드 실행 취약성 Microsoft Office Excel CVE-2024-49029 Microsoft Excel 원격 코드 실행 취약성 Microsoft Office Excel CVE-2024-49028 Microsoft Excel 원격 코드 실행 취약성 Microsoft Office Excel CVE-2024-49027 Microsoft Excel 원격 코드 실행 취약성 Microsoft Office Excel CVE-2024-49026 Microsoft Excel 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-49025 Microsoft Edge(Chromium 기반) 정보 공개 취약성 Microsoft Edge (Chromium-based) CVE-2024-49023 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 SQL Server CVE-2024-49021 Microsoft SQL Server 원격 코드 실행 취약성 Role: Windows Active Directory Certificate Services CVE-2024-49019 Active Directory 인증서 서비스 권한 상승 취약성 SQL Server CVE-2024-49018 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49017 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49016 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49015 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49014 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49013 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49012 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49011 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49010 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49009 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49008 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49007 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49006 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49005 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49004 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49003 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49002 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49001 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-49000 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48999 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48998 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48997 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48996 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48995 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48994 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-48993 SQL Server Native Client 원격 코드 실행 취약성 Windows Secure Kernel Mode CVE-2024-43646 Windows 보안 커널 모드 권한 상승

취약성 Windows Defender Application Control (WDAC) CVE-2024-43645 WDAC(Windows Defender Application Control) 보안 기능 바이패스 취약성 Windows CSC Service CVE-2024-43644 Windows 클라이언트 쪽 캐싱 권한 상승 취약성 Windows USB Video Driver CVE-2024-43643 Windows USB 비디오 클래스 시스템 드라이버 권한 상승 취약성 Windows SMB CVE-2024-43642 Windows SMB 서비스 거부 취약성 Windows Registry CVE-2024-43641 Windows 레지스트리 권한 상승 취약성 Windows Secure Kernel Mode CVE-2024-43640 Windows 커널 모드 드라이버 권한 상승 취약성 Windows Kerberos CVE-2024-43639 Windows KDC Proxy Remote Code Execution Vulnerability Windows USB Video Driver CVE-2024-43638 Windows USB 비디오 클래스 시스템 드라이버 권한 상승 취약성 Windows USB Video Driver CVE-2024-43637 Windows USB 비디오 클래스 시스템 드라이버 권한 상승 취약성 Windows DWM Core Library CVE-2024-43636 Win32k 권한 상승 취약성 Windows Telephony Service CVE-2024-43635 Windows 전화 통신 서비스 원격 코드 실행 취약성 Windows USB Video Driver CVE-2024-43634 Windows USB 비디오 클래스 시스템 드라이버 권한 상승 취약성 Role: Windows Hyper-V CVE-2024-43633 Windows Hyper-V 서비스 거부 취약성 Windows Secure Kernel Mode CVE-2024-43631 Windows 보안 커널 모드 권한 상승 취약성 Windows Kernel CVE-2024-43630 Windows 커널 권한 상승 취약성 Windows DWM Core Library CVE-2024-43629 Windows DWM 핵심 라이브러리 권한 상승 취약성 Windows Telephony Service CVE-2024-43628 Windows 전화 통신 서비스 원격 코드 실행 취약성 Windows Telephony Service CVE-2024-43627 Windows 전화 통신 서비스 원격 코드 실행 취약성 Windows Telephony Service CVE-2024-43626 Windows 전화 통신 서비스 권한 상승 취약성 Windows VMSwitch CVE-2024-43625 Microsoft Windows VMSwitch 권한 상승 취약성 Role: Windows Hyper-V CVE-2024-43624 Windows Hyper-V 공유 가상 디스크 권한 상승 취약성 Windows NT OS Kernel CVE-2024-43623 Windows NT OS 커널 권한 상승 취약성 Windows Telephony Service CVE-2024-43622 Windows 전화 통신 서비스 원격 코드 실행 취약성 Windows Telephony Service CVE-2024-43621 Windows 전화 통신 서비스 원격 코드 실행 취약성 Windows Telephony Service CVE-2024-43620 Windows 전화 통신 서비스 원격 코드 실행 취약성 Azure Database for PostgreSQL CVE-2024-43613 Azure Database for PostgreSQL 유연한 서버 확장 권한 상승 취약성 Power BI CVE-2024-43612 Power BI 보고 서버 스푸핑 취약성 Azure CycleCloud CVE-2024-43602 Azure CycleCloud 원격 코드 실행 취약성 Visual Studio Code CVE-2024-43601 Linux 용 Visual Studio Code 원격 코드 실행 취약성 Remote Desktop Client CVE-2024-43599 원격 데스크톱 클라이언트 원격 코드 실행 취약성 LightGBM CVE-2024-43598 LightGBM 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-43596 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-43595 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-43587 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Winlogon CVE-2024-43583 Winlogon 권한 상승 취약성 Windows Remote Desktop CVE-2024-43582 원격 데스크톱 프로토콜 서버 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-43580 Microsoft Edge(Chromium 기반) 스푸핑 취약성 Microsoft Edge (Chromium-based) CVE-2024-43579 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-43578 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-43577 Microsoft Edge(Chromium 기반) 스푸핑 취약성 Microsoft Edge (Chromium-based) CVE-2024-43566 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Windows Update Stack CVE-2024-43530 Windows 업데이트 스택 권한 상승 취약성 Windows Print Spooler Components CVE-2024-43529 Windows 인쇄 스풀러 권한 상승 취약성 Windows Secure Kernel Mode CVE-2024-43528 Windows 보안 커널 모드 권한 상승 취약성 Windows Secure Kernel Mode CVE-2024-43516 Windows 보안 커널 모드 권한 상승 취약성 Windows Kernel CVE-2024-43511 Windows 커널 권한 상승 취약성 .NET and Visual Studio CVE-2024-43499 .NET 및 Visual Studio 서비스 거부 취약성 .NET and Visual Studio CVE-2024-43498 .NET 및 Visual Studio 원격 코드 실행 취약성 Visual Studio Code CVE-2024-43488 Arduino 용 Visual Studio Code 확장 원격 코드 실행 취약성 .NET and Visual Studio CVE-2024-43485 .NET 및 Visual Studio 서비스 거부 취약성 .NET, .NET Framework, Visual Studio CVE-2024-43484 .NET, .NET Framework, Visual Studio 서비스 거부 취약성 .NET, .NET Framework, Visual Studio CVE-2024-43483 .NET, .NET Framework, Visual Studio 서비스 거부 취약성 Power BI CVE-2024-43481 Power BI 보고 서버 스푸핑 취약성 SQL Server CVE-2024-43462 SQL Server Native Client 원격 코드 실행 취약성 SQL Server CVE-2024-43459 SQL Server Native Client 원격 코드 실행 취약성 Windows Registry CVE-2024-43452 Windows

레지스트리 권한 상승 취약성 Windows NTLM CVE-2024-43451 NTLM 해시 공개 스푸핑 취약성 Microsoft Windows DNS CVE-2024-43450 Windows DNS 스푸핑 취약성 Windows USB Video Driver CVE-2024-43449 Windows USB 비디오 클래스 시스템 드라이버 권한 상승 취약성 Windows SMBv3 Client/Server CVE-2024-43447 Windows SMBv3 Server 원격 코드 실행 취약성 Microsoft Virtual Hard Drive CVE-2024-38264 Microsoft VHDX(가상 하드 디스크) 서비스 거부 취약성 SQL Server CVE-2024-38255 SQL Server Native Client 원격 코드 실행 취약성 Online Services CVE-2024-38204 Imagine Cup 사이트 정보 공개 취약성 Windows Package Library Manager CVE-2024-38203 Windows 패키지 라이브러리 관리자 정보 공개 취약성 Windows Update Stack CVE-2024-38202 Windows 업데이트 스택 권한 상승 취약성 Power Platform CVE-2024-38190 Power Platform 정보 공개 취약성 Azure Managed Instance for Apache Cassandra CVE-2024-38175 Azure Managed Instance for Apache Cassandra 권한 상승 취약성 .NET and Visual Studio CVE-2024-38167 .NET 및 Visual Studio 정보 공개 취약성 Microsoft Dataverse CVE-2024-38139 Microsoft Dataverse 권한 상승 취약성 Windows Deployment Services CVE-2024-38138 Windows Deployment Services 원격 코드 실행 취약성 Microsoft Edge (Chromium-based) CVE-2024-11117 Chromium: CVE-2024-11117 Inappropriate implementation in FileSystem Microsoft Edge (Chromium-based) CVE-2024-11116 Chromium: CVE-2024-11116 Inappropriate implementation in Paint Microsoft Edge (Chromium-based) CVE-2024-11115 Chromium: CVE-2024-11115 Insufficient policy enforcement in Navigation Microsoft Edge (Chromium-based) CVE-2024-11114 Chromium: CVE-2024-11114 Inappropriate implementation in Views Microsoft Edge (Chromium-based) CVE-2024-11113 Chromium: CVE-2024-11113 Use after free in Accessibility Microsoft Edge (Chromium-based) CVE-2024-11112 Chromium: CVE-2024-11112 Use after free in Media Microsoft Edge (Chromium-based) CVE-2024-11111 Chromium: CVE-2024-11111 Inappropriate implementation in Autofill Microsoft Edge (Chromium-based) CVE-2024-11110 Chromium: CVE-2024-11110 Inappropriate implementation in Blink Microsoft Edge (Chromium-based) CVE-2024-10827 Chromium: CVE-2024-10827 Serial 에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-10826 Chromium: CVE-2024-10826 Family Experiences 에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-10488 Chromium: CVE-2024-10488 WebRTC 에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2024-10487 Chromium: CVE-2024-10487: Dawn 에서 범위를 벗어난 쓰기 Microsoft Edge (Chromium-based) CVE-2024-10231 Chromium: CVE-2024-10231 V8 에서 유형 혼란 Microsoft Edge (Chromium-based) CVE-2024-10230 Chromium: CVE-2024-10230 V8 에서 유형 혼란 Microsoft Edge (Chromium-based) CVE-2024-10229 Chromium: CVE-2024-10229 확장에서 부적절한 구현 Microsoft Azure Kubernetes Service CVE-2024-0132 NVIDIA: CVE-2024-0132 컨테이너 도구 키트 1.16.1 이하 검사 시간 사용 시간 취약성 Microsoft Edge (Chromium-based) CVE-2023-6112 Chromium: CVE-2023-6112 탐색에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2023-5997 Chromium: CVE-2023-5997 가비지 수집에서 UaF(Use after free) Microsoft Edge (Chromium-based) CVE-2023-36026 Microsoft Edge(Chromium 기반) 스푸핑 취약성 Microsoft Edge (Chromium-based) CVE-2023-36008 Microsoft Edge(Chromium 기반) 원격 코드 실행 취약성 Azure SDK CVE-2020-16971 Java 용 Azure SDK 보안 기능 우회 취약성 Microsoft Windows CVE-2016-3352 Windows 정보 유출 취약성 WinVerifyTrust Signature Verification CVE-2013-3900 WinVerifyTrust 서명 유효 취약성 ㅁ작성 :위협분석단 취약점분석팀

바로가기

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-11-18)

[미리보기]

2024-12-09 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Progress Kemp LoadMaster contains an OS command injection vulnerability that allows an unauthenticated, remote attacker to access the system through the LoadMaster management interface, enabling arbitrary system command execution. 2024-11-18 Progress Kemp LoadMaster OS Command Injection Vulnerability Progress CVE-2024-1212 2024-12-09 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Additionally, management interface for affected devices should not be exposed to untrusted networks, including the internet. Palo Alto Networks PAN-OS contains an authentication bypass vulnerability in the web-based management interface for several PAN-OS products, including firewalls and VPN concentrators. 2024-11-18 Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability Palo Alto Networks CVE-2024-0012 2024-12-09 Apply mitigations per vendor

instructions or discontinue use of the product if mitigations are unavailable. Additionally, the management interfaces for affected devices should not be exposed to untrusted networks, including the internet. Palo Alto Networks PAN-OS contains an OS command injection vulnerability that allows for privilege escalation through the web-based management interface for several PAN products, including firewalls and VPN concentrators. 2024-11-18 Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability Palo Alto Networks CVE-2024-9474

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