프로젝트 글래스윙 공개 취약점 신속 패치 권고[경계]

<'26.06.16(화), 의료정보보호센터>

□ 개요

○ 최근 미국 앤트로픽사는 '프로젝트 글래스윙(Project Glasswing) 추진 과정에서 발굴한 주요 오픈소스 소프트웨어 취약점에 대해 검증과 오픈소스 패치 절차를 거친 후, 일부 취약점 정보를 공개하여 보안 패치를 권고

□ 주요내용

○ 이번 공개 된 취약점에는 국내외 정보시스템에서 활용 가능성이 있는 주요 오픈소스 구성요소가 포함되어 있음

○ 기관은 관련 오픈소스 구성요소의 사용 여부와 취약 버전 해당 여부를 점검하고, 영향이 확인될 경우 최신 보안패치를 신속히 적용 필요

○ 영향받는 대상

항목	취약점 대상
주요 오픈소스	nginx, jq, MapServer, Temporal, wolfSSL, ImageMagick, MinIO, Nomad, libyang, CraftCMS, Mastodon, Ghost, GitoxideLabs, Junrar, FreeRDP 등

○ 주요 보안취약 오픈소스 목록

순번	오픈소스명	분류	설명
1	nginx	웹서버	홈페이지나 웹 서비스를 운영하고 접속을 중계하는 웹서버 프로그램
2	jq	데이터처리	시스템에서 주고받는 복잡한 데이터를 필요한 내용만 골라보기 쉽게 정리하는 도구
3	MapServer	지도 서비스	인터넷 지도나 위치정보 서비스를 만들 때 쓰는 지도 서비스 프로그램
4	Temporal	업무 자동화	여러 단체의 업무 처리를 자동으로 실행하고, 실패하면 이어서 처리하도록 돕는 플랫폼
5	wolfSSL	암호화 통신	인터넷 통신을 암호화해 안전하게 주고받도록 해주는 프로그램
6	ImageMagick	이미지 처리	이미지 파일을 변환·편집하거나 크기를 조정할 때 쓰는 이미지 처리 도구

순번	오픈소스명	분류	설명
7	MinIO	파일저장	사진·문서·백업파일 등 대용량 데이터를 서버에 저장·관리하는 저장소 프로그램
8	Nomad	서버 운영관리	여러 서버에 프로그램을 자동 배치·실행·관리하는 서버 운영관리 도구
9	Libyang	네트워크 설정	네트워크 장비 설정 정보를 정해진 형식으로 읽고 처리하는 프로그램
10	CraftCMS	홈페이지 관리	기관 홈페이지나 웹사이트 콘텐츠를 관리하는 웹사이트 관리 프로그램
11	Mastodon	SNS 서비스	자체적으로 운영할 수 있는 분산형 SNS 서비스 프로그램
12	Ghost	게시 플랫폼	블로그·뉴스레터·콘텐츠 사이트를 운영하는 웹사이트 게시 플랫폼
13	gitoxide	Git 처리	Git 저장소를 읽고 처리하는 프로그램
14	junrar	압축 해제	RAR 압축파일을 읽고 풀 때 쓰는 JAVA용 압축 해제 프로그램
15	FreeRDP	원격접속	원격 PC나 서버 화면에 접속할 때 쓰는 원격 데스크톱 접속 프로그램

○ 주요 CVE・GHSA 공개 취약점

ID	분류	설명		영향도
CVE-2026-27654	NGINX	힙 버퍼 오버플로우	별칭 지시문을 사용하는 DAV 복사/이동 시 힙 버퍼 오버플로우 발생, 대상 URL이 별칭 길이보다 짧으면 ngx_http_map_uri_to_path 버퍼 계산에서 size_t 언더플로우 발생하고, ngx_copy 오버플로우 발생	High
		임의 파일 쓰기	nginx WebDAV 모듈에서 인증되지 않은 원격 파일 쓰기 가능	Critical
CVE-2026-32316	jq	힙 버퍼 오버플로우	문자열 연결 중 정수 오버플로우로 memcpy 기반 힙 버퍼 오버플로우 발생	Medium
CVE-2026-33721	MapServer	힙 버퍼 오버플로우	SLD 범주화 임계값 구문 분석에서 힙 버퍼 오버 플로우가 발생하는 이유는 재할당 가드에서 잘못된 카운터 변수에 기인	Medium
CVE-2026-5199	Temporal	접근 제어 오류	동일 클러스터 내 워크플로우의 네임스페이스 간 조작(삭제 포함)	Critical
CVE-2026-5446	wolfSSL	암호화 실패	wolfSSL의 TLS 1.2 레코드 암호화에서 ARIA-GCM nonce 재사용	High
CVE-2026-5447	wolfSSL	힙 버퍼 오버플로우	설명 없음	Medium
CVE-2026-5448	wolfSSL	힙 버퍼 오버플로우	wolfSSL_X509 notAfter / wolfSSL_X509_notBefore의 2바이트 힙 오버플로우 발생	Medium

ID	분류	설명		영향도
CVE-2026-5466	wolfSSL	서명 우회	ECCSI 범용 서명 위조 가능	High
CVE-2026-5477	wolfSSL	정수 오버플로우	CMAC 32비트 totalsz 랩어라운드 접두사 치환 위조	High
CVE-2026-5479	wolfSSL	암호화 실패	wolfSSL evp chacha20 Poly1305 태그 미확인	High
CVE-2026-5500	wolfSSL	암호화 실패	AEAD GCM 인증 태그 길이를 제대로 검증	High
CVE-2026-5501	wolfSSL	인증서 검증 오류	wolfSSL x.509 verity cert Leaf 시그니처 인증	High
CVE-2026-5503	wolfSSL	힙 버퍼 오버플로우	wolfSSL ech heap buffer overflow via publicname sni poi	High
CVE-2026-7474	Nomad	경로 탐색	nomad : 클라이언트 / hostvolumemanager/ host_volume_plugin.go:229에서 경로 탐색 오류 발생	Critical
GHSA-9f49-8x56-jmjc	Libyang	사용 후 무료	XML 데이터 파싱 중 메타데이터 목록 관리에서 잘못된 목록 헤드 포인터 업데이트로 인해 사용 후 해제(Use-after-free) 쓰기 오류 발생	Medium
GHSA-cc7p-2j3x-x7xf	Craft CMS	권한 상승	UserController->actionImpersonateWithToken()을 통한 권한 상승/우회	High
GHSA-chgx-jx3p-rf73	Mastodon	시그니처 바이패스	JSON-LD 명명 그래프 재구성을 통한 LD 서명 우회	High
GHSA-crr4-7rm4-8gpw	Mastodon	SSRF	Mastodon에서 IPv6 지정되지 않은 주소(::)를 통한 SSRF 웅회	High
GHSA-f26g-jm89-4g65	GitoxideLabs /gitoide	원격 코드 실행(RCE)	악성 저장소의 Git 서브모듈을 업데이트할 때 원격 코드 실행(RCE) 발생	High
GHSA-j273-m5qq-6825	junrar	경로 탐색	역슬래시 경로 탐색으로 인한 임의 파일 쓰기	Medium
GHSA-mpxh-8fq3-x8mh	FreeRDP	힙 버퍼 오버플로우	cliprdr_main.c:547에서 힙 버퍼 오버플로우 발생	High
GHSA-w52v-v783-gw97	Ghost	SQL 인젝션	Content API에 대한 SQL 인젝션 공격	Critical
GHSA-x9h5-r9v2-vcww	ImageMagick	힙 버퍼 오버플로우	CopyMagicString을 사용하여 경계 검사를 하지 않고, MVG 패턴을 랜더링 할 때 힙 버퍼 오버플로우 발생	High
GHSA-xh8f-g2qw-gcm7	MinIO	경로 탐색	minio: cmd/xl-storage.go:3194-3218 (싱크) 및 cmd/storage-rest-server.go:1287-1326 (핸들러)에서 경로 탐색 오류 발생	Medium

□ 대응방안

○ 공개된 취약점은 국내외 서비스·시스템에서 널리 활용되는 오픈소스로 취약점이 포함된 제품 또는 소프트웨어를 확인하여 최신 보안 패치를 적용

취약점	제품명	영향 받는 버전	해결 버전
CVE-2026-27654	NGINX Open Source	1.29.6 이하	1.29.7 이상
CVE-2026-27654	NGINX Plus	R34 이하	R35 이상
CVE-2026-32316	jq	1.8.1 이하	1,8,2 이상
CVE-2026-33721	MapServe	8.6.0 이하	8.6.1 이상
CVE-2026-5199	Temporal	1.29.4 이하 1.30.2 이하	1.29.5 이상, 1.30.3 이상
CVE-2026-5446	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5447	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5448	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5466	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5477	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5479	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5500	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5501	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-5503	wolfSSL	5.9.1 미만	5.9.1 이상
CVE-2026-7474	Nomad	5.2.5 미만	5.2.6 이상
GHSA-9f49-8x56-jmjc (CVE-2026-41401)	Libyang	5.2.0 ~ 5.2.5	5.2.6 이상
GHSA-cc7p-2j3x-x7xf (CVE-2026-32267)	CraftCMS	4.0.0-RC1 ~ 4.17.5 5.0.0-RC1 ~ 5.9.11	4.17.6 이상 5.9.12 이상
GHSA-chgx-jx3p-rf73 (CVE-2026-46349)	Mastodon	4.3.0 ~ 4.5.9	4.3.23 4.4.17 4.5.10 이상
GHSA-crr4-7rm4-8gpw	Mastodon	4.3.0 ~ 4.5.9	4.3.23 4.4.17 4.5.10 이상
GHSA-f26g-jm89-4g65	GitoxideLabs/gitoide	gix 0.31.0 ~ 0.82.x (0.83.0 미만)	0.83.0 이상
GHSA-j273-m5qq-6825 (CVE-2026-28208)	junrar	7.5.8 미만	7.5.8 이상
GHSA-mpxh-8fq3-x8mh (CVE-2026-45700)	FreeRDP	3.26.0 미만	3.26.0 이상
GHSA-w52v-v783-gw97 (CVE-2026-26980)	Ghost	3.24.0 ~ 6.19.0	6.19.1 이상
GHSA-x9h5-r9v2-vcww (CVE-2026-33901)	ImageMagick	7.1.2-19 미만 6.9.13-44 미만	7.1.2-19 이상 6.9.13-44 이상
GHSA-xh8f-g2qw-gcm7 (CVE-2026-42600)	MinIO	2026-04-14 이전 버전	2026-04-14T21-32-45Z 이상

□ 기타 사항

○ 이상징후 발견시 의료정보보호센터(www.hisc.or.kr)로 신고하여 주시기 바랍니다.

○ (연락처) 의료정보보호센터

- email: cert@hisac.or.kr
- Tel: 02-6360-6283