Git Buffer Overflow 취약점 공지

이 문서는 Atlassian제품에 영향을 미치는 Git Buffer Overflow 관련 보안 취약점 공지와 조치 사항에 대한 정보를 공유하기 위해 작성되었다.

요약	Git Buffer Overflow in Multiple Products
보안 안내	2023. 2. 17. 10:00 AM PDT (Pacific Time, -7 hours)
영향을 받는 제품	• Bitbucket Server and Data Center • Bamboo Server and Data Center • Fisheye • Crucible • Sourcetree **Atlassian Cloud 사이트는 영향을 받지 않습니다.** 수정 사항이 Atlassian Cloud 사이트에 배포되었습니다. Bitbucket.org 또는 atlassian.net 도메인을 통해 Atlassian 사이트에 액세스하는 경우 Atlassian Cloud 사이트입니다.
CVE ID	CVE-2022-41903 CVE-2022-23521

Git Overflow 보안 업데이트 권고

보안 취약점 요약

이 취약점은 악의적인 공격자가 Git 클라이언트를 통해 Git 저장소에 악성 코드를 주입하여 공격하는 것이 가능하게 되어 있습니다. 취약점을 악용하면 Git 클라이언트를
사용하여 저장소의 권한을 무력화하거나 사용자의 컴퓨터에서 코드를 실행시킬 수 있습니다. 이러한 취약점으로부터 사용자는 가능한 빠른 시일 내에 해당 업데이트를 적용해야 합니다.

보안 취약 코드

- CVE-2022-41903
  - git archive노출로 힙 오버플, 원격코드 실행 취약점
  - CVE-2022-41903
- CVE-2022-23521

- gitattributes 다중 오버플로 원격코드 실행 취약점
- CVE-2022-23521

주요 내용 및 영향 받는 버전 및 대응방안

- https://github.com/git/git/security/advisories/GHSA-475x-2q3q-hvwq
- https://github.com/git/git/security/advisories/GHSA-c738-c5qq-xg89

제품 별 대처 방안

취약 여부

- CVE-2022-41903
  - git log에는 --format 지정자와 함께 임의 형식을 사용하여 커밋을 표시하는 기능이 있습니다. 이 기능은 또한 내보내기-하위 Git 속성을 통해 Git 아카이브에 노출됩니다.
    패딩 연산자(예: %<(, %<|(, %>)를 처리할 때 pretty.c::format_and_pad_commit()에서 정수 오버플로가 발생할 수 있으며, 여기서 size_t가 int로 부적절하게 저장된 다음 후속 memcpy() 호출에 오프셋으로 추가됩니다. 이 오버플로는 커밋 포맷 기계를 호출하는 명령(예: git log --format=...)을 실행하는 사용자에 의해 직접 트리거될 수 있습니다. 또한 Git 아카이브 동안 저장소 내 파일 내부의 형식 지정자를 확장하는 export-subst 메커니즘을 통해 Git 아카이브를 통해 간접적으로 트리거될 수도 있습니다. 이 정수 오버플로로 인해 임의의 힙 쓰기가 발생하여 원격 코드가 실행될 수 있습니다.
- CVE-2022-23521
  - git 속성은 경로에 대한 속성을 정의할 수 있는 메커니즘입니다. 이러한 특성은 파일 패턴 집합과 이 패턴과 일치하는 경로에 대해 설정해야 하는 특성을 포함하는 .git 특성 파일을 저장소에 추가하여 정의할 수 있습니다.
    git 속성을 구문 분석할 때, 엄청난 수의 경로 패턴이 있거나 단일 패턴에 대해 엄청난 수의 속성이 있거나 선언된 속성 이름이 클 때 여러 정수 오버플로가 발생할 수 있습니다. 이러한 오버플로는 커밋 기록의 일부인 조작된 .git 특성 파일을 통해 트리거될 수 있습니다. Git는 파일에서 Git 특성을 구문 분석할 때 2KB보다 긴 줄을 자동으로 분할하지만 인덱스에서 구문 분석할 때는 분할하지 않습니다. 따라서 실패 모드는 파일이 작업 트리에 있는지, 인덱스에 있는지 또는 둘 다에 따라 달라집니다. 이 정수 오버플로로 인해 임의의 힙 읽기 및 쓰기가 발생하여 원격 코드가 실행될 수 있습니다.

Bitbucket 서버 및 데이터 센터

Bitbucket Server 및 Bitbucket Data Center 의 모든 버전이 영향을 받습니다.

패치 권장 사항

Git 구성	추천
Git을 직접 제공하는 고객의 경우	Atlassian은 고객이 사용 가능한 최신 패치 및 지원 버전의 Git으로 업그레이드할 것을 권장합니다. Git의 패치 버전을 지원하는지 확인하려면 Bitbucket 버전의 지원되는 플랫폼 페이지를 참조하세요 . Bitbucket Server 및 Data Center < 7.9 버전을 사용하는 고객은 Git의 패치 버전을 지원하려면 Bitbucket을 최신 버전으로 업그레이드해야 합니다. 그러나 Bitbucket 7.6을 실행하는 고객 의 경우 Bitbucket 팀은 Git v2.30.7이 작동하는지 테스트하고 확인했습니다.
Bitbucket Docker 이미지를 사용하는 고객의 경우	Bitbucket에 대한 지원 수명 주기의 모든 이미지가 Git 패치 버전을 사용하도록 업데이트되었습니다. 최신 변경 사항을 가져오려면 이미지를 다시 다운로드하십시오. 마찬가지로 Bitbucket 이미지를 해시에 고정하는 고객은 해당 이미지 태그와 연결된 최신 해시 버전으로 업데이트해야 합니다.
Windows용 Git을 사용하는 고객의 경우	Bitbucket 팀은 Git v2.39.x에 대한 지원을 추가하는 버전 v7.21.9를 출시했습니다. 사용 가능한 최신 패치 및 지원 버전의 Git으로 업데이트하십시오. 현재 Git for Windows는 이러한 취약점에 대한 수정 사항을 백포트 할 계획이 없습니다 .

Bamboo 서버 및 데이터 센터

Bamboo의 모든 버전이 영향을 받습니다.

패치 권장 사항

Git 구성	추천

Git을 직접 제공하는 고객의 경우	Atlassian은 고객이 Bamboo 서버 및 원격 에이전트에서 Git을 사용 가능한 최신 패치 및 지원 버전으로 업데이트할 것을 권장합니다. Git의 패치 버전을 지원하는지 확인하려면 Bamboo 버전의 지원 플랫폼 페이지를 참조하십시오 .
Bamboo Docker 이미지를 사용하는 고객의 경우	지원 수명 주기의 모든 이미지는 Git 패치 버전을 사용하도록 업데이트되었습니다. 최신 변경 사항을 가져오려면 이미지를 다시 다운로드하십시오. 마찬가지로 Bamboo 이미지를 해시에 고정하는 고객은 해당 이미지 태그와 연결된 최신 해시 버전으로 업데이트해야 합니다.
Elastic Bamboo를 사용하는 고객의 경우	새로운 AMI는 곧 출시될 Bamboo 9.1.3 릴리스의 지원되는 지역에서 Linux 및 Windows용 패치된 Git 버전으로 준비되었습니다. 출시를 기다리기 싫은 고객은 기존 이미지 구성 화면의 이미지 시작 스크립트에 Git을 업데이트하는 줄을 추가하거나 공식 출시 전에 AMI를 다운로드하여 사용할 수 있습니다 .
Windows용 Git을 사용하는 고객의 경우	최신 버전의 Windows용 Git으로 업데이트하세요. 현재 Git for Windows는 이러한 취약점에 대한 수정 사항을 백포트 할 계획이 없습니다 .

Fisheye 서버

Fisheye의 모든 버전이 영향을 받습니다.

패치 권장 사항

Git 구성	추천
Git을 직접 제공하는 고객의 경우	Atlassian은 고객이 사용 가능한 최신 패치 및 지원 버전의 Git으로 업그레이드할 것을 권장합니다. Git의 패치 버전을 지원하는지 확인하려면 Fisheye 버전의 지원되는 플랫폼 페이지를 참조하십시오 .
Fisheye Docker 이미지를 사용하는 고객의 경우	지원 수명 주기의 모든 이미지는 Git 패치 버전을 사용하도록 업데이트되었습니다. 최신 변경 사항을 가져오려면 이미지를 다시 다운로드하십시오. 마찬가지로 Fisheye 이미지를 해시에 고정하는 고객은 해당 이미지 태그와 연결된 최신 해시 버전으로 업데이트해야 합니다.
Windows용 Git을 사용하는 고객의 경우	최신 버전의 Windows용 Git으로 업데이트하세요. 현재 Git for Windows는 이러한 취약점에 대한 수정 사항을 백포트 할 계획이 없습니다 .

Crucible 서버

Crucible의 모든 버전이 영향을 받습니다.

패치 권장 사항

Git 구성	추천
Git을 직접 제공하는 고객의 경우	Atlassian은 고객이 사용 가능한 최신 패치 및 지원 버전의 Git으로 업그레이드할 것을 권장합니다. Git의 패치 버전을 지원하는지 확인하려면 Crucible 버전의 지원 플랫폼 페이지를 참조하세요 .
Crucible Docker 이미지를 사용하는 고객의 경우	지원 수명 주기의 모든 이미지는 Git 패치 버전을 사용하도록 업데이트되었습니다. 최신 변경 사항을 가져오려면 이미지를 다시 다운로드하십시오. 마찬가지로 Crucible 이미지를 해시에 고정하는 고객은 해당 이미지 태그와 연결된 최신 해시 버전으로 업데이트해야 합니다.
Windows용 Git을 사용하는 고객의 경우	최신 버전의 Windows용 Git으로 업데이트하세요. 현재 Git for Windows는 이러한 취약점에 대한 수정 사항을 백포트 할 계획이 없습니다 .

Sourcetree

Mac 및 Windows용 Sourcetree의 모든 버전은 취약합니다.

고정 버전

Sourcetree 팀은 다음 제품 릴리스 버전을 위해 포함된 Git 바이너리를 v2.39.1로 업데이트하기 위해 적극적으로 노력하고 있습니다.

- 맥: v4.2.2

- 윈도우: v3.4.12

완화

Sourcetree 팀이 포함된 Git 바이너리를 업데이트하는 동안 고객은 Sourcetree를 전환하여 패치된 시스템 Git 버전을 사용하는 것이 좋습니다 .

해결 방안

가장 완벽한 해결 방법은 가장 최근에 게시된 패치 버전으로 Git을 업그레이드하는 것입니다.

- 이렇게 하는 것이 실용적이지 않은 경우 리포지토리에서 git 아카이브를 사용하지 않도록 설정합니다.
  git daemon을 통해 git 아카이브를 노출하는 경우 git config --global daemon.uploadArch false를 실행하여 비활성화합니다.
  그렇지 않은 경우 신뢰할 수 없는 리포지토리에서 직접 git 아카이브를 실행하지 마십시오.

영향을 받는 버전

- v2.30.6, v2.31.5, v2.32.4, v2.33.5, v2.34.5, v2.35.5, v2.36.3, v2.37.4, v2.38.2, v2.39.

패치 버전

- v2.30.7, v2.31.6, v2.32.5, v2.33.6, v2.34.6, v2.35.6, v2.36.4, v2.37.5, v2.38.3, v2.39.1
