제품 보안

Enterprise applications

NetApp
May 03, 2024

목차

제품 보안

VMware vSphere용 ONTAP 툴

ONTAP Tools for VMware vSphere의 소프트웨어 엔지니어링에서는 다음과 같은 보안 개발 활동을 활용합니다.

- * 위협 모델링. * 위협 모델링의 목적은 소프트웨어 개발 수명 주기 초기에 피처, 부품 또는 제품의 보안 결함을 발견하기 위한 것입니다. 위협 모델은 응용 프로그램의 보안에 영향을 주는 모든 정보의 구조적 표현입니다. 본질적으로 보안 렌즈를 통해 응용 프로그램과 환경을 볼 수 있습니다.
- * DAST(Dynamic Application Security Testing). * 이 기술은 실행 중인 응용 프로그램의 취약한 상태를 감지하도록 설계되었습니다. DAST는 웹 활성화 애플리케이션의 노출된 HTTP 및 HTML 인터페이스를 테스트합니다.
- * 타사 코드 통화. * 오픈 소스 소프트웨어(OSS)를 통한 소프트웨어 개발의 일환으로 제품에 통합된 OSS와 관련된 보안 취약점을 해결해야 합니다. 이는 새로운 OSS 버전에 새로 발견된 취약점이 언제든지 보고될 수 있기 때문에 지속적인 노력입니다.
- * 취약성 검사. * 취약성 검사의 목적은 NetApp 제품이 고객에게 공개되기 전에 NetApp 제품의 알려진 공통 보안 취약점을 감지하는 것입니다.
- * 침투 테스트 * 침투 테스트는 시스템, 웹 응용 프로그램 또는 네트워크를 평가하여 공격자가 악용할 수 있는 보안 취약점을 찾는 프로세스입니다. NetApp의 침투 테스트(펜 테스트)는 승인되고 신뢰할 수 있는 타사 기업의 그룹에 의해 수행됩니다. 이러한 테스트 범위에는 정교한 악용 방법이나 도구를 사용하는 악의적인 침입자나 해커에 유사한 응용 프로그램 또는 소프트웨어에 대한 공격이 포함됩니다.

제품 보안 기능

VMware vSphere용 ONTAP 툴에는 각 릴리즈에 다음과 같은 보안 기능이 포함되어 있습니다.

- * 로그인 배너. * SSH는 기본적으로 비활성화되어 있으며 VM 콘솔에서 활성화된 경우 1회만 로그인할 수 있습니다. 사용자가 로그인 프롬프트에 사용자 이름을 입력하면 다음 로그인 배너가 표시됩니다.

  경고:* 이 시스템에 대한 무단 액세스는 금지되며 법률로 기소됩니다. 이 시스템에 액세스하면 무단 사용이 의심되는 경우 사용자의 조치를 모니터링할 수 있다는 데 동의하는 것입니다.

  사용자가 SSH 채널을 통한 로그인을 완료하면 다음 텍스트가 표시됩니다.

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * 역할 기반 액세스 제어(RBAC). * 두 가지 유형의 RBAC 컨트롤이 ONTAP 도구에 연결되어 있습니다.
  - 기본 vCenter Server 권한

- vCenter 플러그인별 권한 자세한 내용은 을 참조하십시오 "이 링크".

- * 암호화된 통신 채널. * 모든 외부 통신은 TLS 버전 1.2를 사용하여 HTTPS를 통해 이루어집니다.
- * 최소 포트 노출. * 필요한 포트만 방화벽에서 열립니다.

  다음 표에서는 열려 있는 포트의 세부 정보를 설명합니다.

TCP v4/V6 포트 번호	방향	기능
8143	인바운드	REST API용 HTTPS 연결
8043을 참조하십시오	인바운드	HTTPS 연결
9060입니다	인바운드	HTTPS 연결 https 연결을 통한 SOAP에 사용됩니다 클라이언트가 ONTAP 도구 API 서버에 연결할 수 있도록 하려면 이 포트를 열어야 합니다.
22	인바운드	SSH(기본적으로 비활성화됨)
9080입니다	인바운드	HTTPS 연결 - VP 및 SRA - 루프백에서만 내부 연결
9083	인바운드	HTTPS 연결 - VP 및 SRA https 연결을 통한 SOAP에 사용됩니다
1162	인바운드	VP SNMP 트랩 패킷입니다
1527년	내부 전용	Derby 데이터베이스 포트, 이 컴퓨터와 자체 사이에서만, 외부 연결은 허용되지 않음 — 내부 연결만
443	양방향	ONTAP 클러스터에 연결하는 데 사용됩니다

- * CA(인증 기관) 서명 인증서 지원. * VMware vSphere용 ONTAP 툴은 CA 서명 인증서를 지원합니다. 자세한 내용은 다음을 참조하십시오 "KB 문서를 참조하십시오" 를 참조하십시오.
- * 감사 로깅. * 지원 번들은 다운로드할 수 있으며 매우 자세히 설명되어 있습니다. ONTAP 도구는 모든 사용자 로그인 및 로그아웃 활동을 별도의 로그 파일에 기록합니다. VASA API 호출은 전용 VASA 감사 로그(로컬 CXF.log)에 기록됩니다.
- 암호 정책 * 다음 암호 정책을 따릅니다.
  - 암호는 로그 파일에 기록되지 않습니다.
  - 암호는 일반 텍스트로 전달되지 않습니다.
  - 암호는 설치 과정 중에 구성됩니다.
  - 암호 기록은 구성 가능한 매개 변수입니다.
  - 최소 암호 사용 기간은 24시간으로 설정됩니다.
  - 암호 필드에 대한 자동 완성 기능이 비활성화됩니다.
  - ONTAP 도구는 SHA256 해싱을 사용하여 저장된 모든 자격 증명 정보를 암호화합니다.

SnapCenter 플러그인 VMware vSphere

NetApp SnapCenter Plug-in for VMware vSphere 소프트웨어 엔지니어링은 다음과 같은 안전한 개발 활동을 사용합니다.

- * 위협 모델링. * 위협 모델링의 목적은 소프트웨어 개발 수명 주기 초기에 피처, 부품 또는 제품의 보안 결함을 발견하기 위한 것입니다. 위협 모델은 응용 프로그램의 보안에 영향을 주는 모든 정보의 구조적 표현입니다. 본질적으로 보안 렌즈를 통해 응용 프로그램과 환경을 볼 수 있습니다.
- * DAST(Dynamic Application Security Testing). * 실행 상태의 응용 프로그램에서 취약한 상태를 감지하도록 설계된 기술입니다. DAST는 웹 활성화 애플리케이션의 노출된 HTTP 및 HTML 인터페이스를 테스트합니다.
- * 타사 코드 통화. * 소프트웨어를 개발하고 오픈 소스 소프트웨어(OSS)를 사용하는 과정에서 제품에 통합된 OSS와 관련된 보안 취약점을 해결하는 것이 중요합니다. 이는 항상 OSS 구성 요소 버전에 새로 발견된 취약점이 보고될 수 있기 때문에 지속적으로 발생하는 것입니다.
- * 취약성 검사. * 취약성 검사의 목적은 NetApp 제품이 고객에게 공개되기 전에 NetApp 제품의 알려진 공통 보안 취약점을 감지하는 것입니다.
- * 침투 테스트 * 침투 테스트는 시스템, 웹 응용 프로그램 또는 네트워크를 평가하여 공격자가 악용할 수 있는 보안 취약점을 찾는 프로세스입니다. NetApp의 침투 테스트(펜 테스트)는 승인되고 신뢰할 수 있는 타사 기업의 그룹에 의해 수행됩니다. 이러한 테스트 범위에는 정교한 악용 방법이나 도구를 사용하는 악의적인 침입자나 해커 같은 응용 프로그램 또는 소프트웨어에 대한 공격이 포함됩니다.
- * 제품 보안 문제의 대응 활동 * 보안 취약성은 사내외에서 발견되며 적시에 해결되지 않을 경우 NetApp의 평판에 심각한 위험을 초래할 수 있습니다. 이 프로세스를 용이하게 하기 위해 PSIRT(Product Security Incident Response Team)는 취약점을 보고 및 추적합니다.

제품 보안 기능

VMware vSphere용 NetApp SnapCenter 플러그인에는 각 릴리즈마다 다음과 같은 보안 기능이 포함되어 있습니다.

- * 제한된 셸 액세스. * SSH는 기본적으로 비활성화되어 있으며, VM 콘솔에서 활성화된 경우에만 1회 로그인이 허용됩니다.
- 로그인 배너에 액세스 경고 * 로그인 프롬프트에 사용자 이름을 입력하면 다음 로그인 배너가 표시됩니다.

  경고:* 이 시스템에 대한 무단 액세스는 금지되며 법률로 기소됩니다. 이 시스템에 액세스하면 무단 사용이 의심되는 경우 사용자의 조치를 모니터링할 수 있다는 데 동의하는 것입니다.

  사용자가 SSH 채널을 통해 로그인을 완료하면 다음 출력이 표시됩니다.

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * 역할 기반 액세스 제어(RBAC). * 두 가지 유형의 RBAC 컨트롤이 ONTAP 도구에 연결되어 있습니다.
  - 기본 vCenter Server 권한

◦ VMware vCenter 플러그인별 권한 자세한 내용은 을 참조하십시오 "역할 기반 액세스 제어(RBAC)".

- * 암호화된 통신 채널. * 모든 외부 통신은 TLS를 사용하여 HTTPS를 통해 이루어집니다.
- * 최소 포트 노출. * 필요한 포트만 방화벽에서 열립니다.

다음 표에는 열려 있는 포트 세부 정보가 나와 있습니다.

TCP v4/V6 포트 번호	기능
8144를 참조하십시오	REST API용 HTTPS 연결
8080	OVA GUI에 대한 HTTPS 연결
22	SSH(기본적으로 비활성화됨)
3306입니다	MySQL(내부 연결에만 해당, 외부 연결은 기본적으로 비활성화됨)
443	Nginx(데이터 보호 서비스)

- * CA(인증 기관) 서명 인증서 지원 * VMware vSphere용 SnapCenter 플러그인은 CA 서명 인증서의 기능을 지원합니다. 을 참조하십시오 "SSL 인증서를 생성 및/또는 VMware vSphere용 SnapCenter 플러그인(SCV)으로 가져오는 방법".
- * 암호 정책 * 다음 암호 정책이 적용됩니다.
  - 암호는 로그 파일에 기록되지 않습니다.
  - 암호는 일반 텍스트로 전달되지 않습니다.
  - 암호는 설치 과정 중에 구성됩니다.
  - 모든 자격 증명 정보는 SHA256 해싱을 사용하여 저장됩니다.
- 기본 운영 체제 이미지**.** 이 제품은 제한된 액세스 및 쉘 액세스가 비활성화된 OVA용 Debian Base OS와 함께 제공됩니다. 이렇게 하면 공격 발생 가능성이 줄어듭니다. 모든 SnapCenter 릴리스 기본 운영 체제는 보안 범위를 극대화하기 위해 최신 보안 패치로 업데이트됩니다.

NetApp은 VMware vSphere 어플라이언스인 SnapCenter 플러그인과 관련된 소프트웨어 기능 및 보안 패치를 개발한 다음 고객에게 번들 소프트웨어 플랫폼으로 배포합니다. 이러한 어플라이언스에는 특정 Linux 하위 운영 체제 종속성 및 NetApp의 독점 소프트웨어가 포함되어 있으므로 하위 운영 체제를 변경하지 않는 것이 좋습니다. 이 경우 NetApp 어플라이언스에 영향을 줄 가능성이 매우 높기 때문입니다. 이는 NetApp의 어플라이언스 지원 기능에 영향을 미칠 수 있습니다. 보안 관련 문제를 해결하기 위해 NetApp은 어플라이언스의 최신 코드 버전을 테스트하고 구축할 것을 권장합니다.

저작권 정보

상표 정보