产品安全性
Enterprise applications

NetApp
May 03, 2024

目录

产品安全性

适用于 **VMware vSphere** 的 **ONTAP** 工具

适用于VMware vSphere的ONTAP工具的软件工程采用以下安全开发活动：

- 威胁建模。 * 威胁建模的目的是在软件开发生命周期早期发现功能，组件或产品中的安全缺陷。威胁模型是影响应用程序安全性的所有信息的结构化表示。从本质上说，它是从安全性角度来看待应用程序及其环境的。
- * 动态应用程序安全测试（ DAST ）。 * 此技术用于检测处于运行状态的应用程序上的易受到攻击的情况。Dast 会测试 Web 应用程序公开的 HTTP 和 HTML 接口。
- * 第三方代码货币。 * 作为开源软件（ OSS ）软件开发的一部分，您必须解决可能与产品中包含的任何 OSS 相关的安全漏洞。这是一项持续努力，因为新的 OSS 版本可能会随时报告新发现的漏洞。
- * 漏洞扫描。 * 漏洞扫描的目的是在 NetApp 产品发布给客户之前检测其常见和已知安全漏洞。
- * 渗透测试。 * 渗透测试是指评估系统， Web 应用程序或网络以发现攻击者可能利用的安全漏洞的过程。NetApp 的渗透测试（笔测试）由一组经过批准且值得信赖的第三方公司执行。其测试范围包括使用复杂的利用方法或工具对与恶意入侵者或黑客类似的应用程序或软件发起攻击。

产品安全功能

适用于VMware vSphere的ONTAP工具在每个版本中都包含以下安全功能。

- 默认情况下， * 登录横幅。 * SSH 处于禁用状态，如果从 VM 控制台启用，则仅允许一次性登录。用户在登录提示符中输入用户名后，将显示以下登录横幅：
- 警告： * 禁止未经授权访问此系统，并将受到法律的起诉。访问此系统即表示您同意，如果怀疑未经授权使用，您的操作可能会受到监控。

  用户通过SSH通道完成登录后、将显示以下文本：

```
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.
```

- * 基于角色的访问控制（ Role-Based Access Control ， RBAC ）。 * ONTAP 工具与两种类型的 RBAC 控制相关联：
  - 原生 vCenter Server 特权
  - vCenter 插件的特定特权。有关详细信息，请参见 "此链接。"。
- * 加密通信通道。 * 所有外部通信均使用 TLS 1.2 版通过 HTTPS 进行。
- * 最小端口暴露。 * 只有必要的端口在防火墙上处于打开状态。

下表介绍了打开的端口详细信息。

TCP v4/v6 端口号	方向	功能
8143.	入站	用于 REST API 的 HTTPS 连接
8043	入站	HTTPS 连接
9060	入站	HTTPS 连接 用于基于 https 的 SOAP 连接 必须打开此端口、客户端才能连接到ONTAP工具API服务器。
22.	入站	SSH （默认为禁用）
9080	入站	HTTPS 连接— VP 和 SRA —仅从环回进行内部连接
9083.	入站	HTTPS 连接— VP 和 SRA 用于基于 https 的 SOAP 连接
1162.	入站	VP SNMP 陷阱数据包
1527.	仅限内部	Derby 数据库端口，仅在此计算机与自身之间，不接受外部连接—仅限内部连接
443.	双向	用于连接到 ONTAP 集群

- * 支持证书颁发机构（ CA ）签名证书。 * 适用于 VMware vSphere 的 ONTAP 工具支持 CA 签名证书。请参见此内容 "知识库文章" 有关详细信息 …
- * 审核日志记录。 * 支持包可以下载，并且非常详细。ONTAP 工具会将所有用户登录和注销活动记录在一个单独的日志文件中。VASA API 调用会记录在专用的 VASA 审核日志（本地 CXF.log ）中。
- * 密码策略。 * 遵循以下密码策略：
  - 密码不会记录在任何日志文件中。
  - 密码不会以纯文本形式传达。
  - 密码是在安装过程本身期间配置的。
  - 密码历史记录是一个可配置的参数。
  - 密码最短期限设置为 24 小时。
  - 已禁用密码字段的自动完成。
  - ONTAP 工具使用 SHA256 哈希对所有存储的凭据信息进行加密。

SnapCenter插件VMware vSphere

适用于VMware vSphere的NetApp SnapCenter 插件软件工程部门使用以下安全开发活动：

- 威胁建模。 * 威胁建模的目的是在软件开发生命周期早期发现功能，组件或产品中的安全缺陷。威胁模型是影响应用程序安全性的所有信息的结构化表示。从本质上说，它是从安全性角度来看待应用程序及其环境的。

- *动态应用程序安全测试(DAST)。*用于检测处于运行状态的应用程序上的易受到攻击的情况的技术。Dast会测试 Web 应用程序公开的 HTTP 和 HTML 接口。
- *第三方代码货币。*在开发软件和使用开源软件(OSS)的过程中、解决可能与您的产品中所含的OSS相关的安全漏洞非常重要。这是一项持续努力、因为OSS组件的版本可能随时报告新发现的漏洞。
- * 漏洞扫描。 * 漏洞扫描的目的是在 NetApp 产品发布给客户之前检测其常见和已知安全漏洞。
- *渗透测试。*渗透测试是指评估系统、Web应用程序或网络以发现攻击者可能利用的安全漏洞的过程。NetApp 的渗透测试（笔测试）由一组经过批准且值得信赖的第三方公司执行。其测试范围包括使用复杂的利用方法或工具对恶意入侵者或黑客等应用程序或软件发起攻击。
- *产品安全事件响应活动。*安全漏洞在公司内部和外部均已发现、如果不及时解决、可能会对NetApp的声誉造成严重风险。为了便于执行此过程、产品安全意外事件响应团队(PSIRT)会报告并跟踪漏洞。

产品安全功能

适用于VMware vSphere的NetApp SnapCenter 插件在每个版本中都包含以下安全功能：

- *限制Shell访问。*默认情况下、SSH处于禁用状态、只有在从VM控制台启用一次性登录后、才允许进行此类登录。
- *登录横幅中显示访问警告。*用户在登录提示符中输入用户名后、将显示以下登录横幅：
- 警告： * 禁止未经授权访问此系统，并将受到法律的起诉。访问此系统即表示您同意，如果怀疑未经授权使用，您的操作可能会受到监控。

  用户通过SSH通道完成登录后、将显示以下输出：

```
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.
```

- * 基于角色的访问控制（ Role-Based Access Control ， RBAC ）。 * ONTAP 工具与两种类型的 RBAC 控制相关联：
  - 本机vCenter Server特权。
  - VMware vCenter插件的特定特权。有关详细信息，请参见 "基于角色的访问控制（ Role-Based Access Control ， RBAC ）"。
- *加密通信通道。*所有外部通信均使用TLS通过HTTPS进行。
- * 最小端口暴露。 * 只有必要的端口在防火墙上处于打开状态。

下表提供了打开的端口详细信息。

TCP v4/v6端口号	功能
8144.	用于 REST API 的 HTTPS 连接
8080	用于OVA GUI的HTTPS连接

TCP v4/v6端口号	功能
22.	SSH (默认情况下处于禁用状态)
3306.	MySQL (仅限内部连接；默认情况下、外部连接处于禁用状态)
443.	nginx (数据保护服务)

- *支持证书颁发机构(CA)签名证书。*适用于VMware vSphere的SnapCenter 插件支持CA签名证书的功能。请参见 "如何创建和/或将SSL证书导入到适用于VMware vSphere的SnapCenter 插件(SCV)"。
- *密码策略。*以下密码策略有效：
  - 密码不会记录在任何日志文件中。
  - 密码不会以纯文本形式传达。
  - 密码是在安装过程本身期间配置的。
  - 所有凭据信息均使用SHA256哈希进行存储。
- *基本操作系统映像。*本产品随附Debian基础操作系统、用于OVA、但访问受限且Shell访问已禁用。这样可以减少攻击占用空间。每个SnapCenter 版本基础操作系统都会更新最新的安全修补程序、以最大限度地提高安全性。

NetApp针对适用于VMware vSphere设备的SnapCenter 插件开发软件功能和安全修补程序、然后将其作为捆绑软件平台发布给客户。由于这些设备包括特定的Linux子操作系统依赖关系以及我们的专有软件、因此NetApp建议您不要更改子操作系统、因为这很可能会影响NetApp设备。这可能会影响NetApp支持此设备的能力。NetApp建议测试和部署我们最新的设备代码版本、因为发布这些代码版本是为了修补任何与安全相关的问题。

版权信息

商标信息