安全2

CVE	影响	原生minio 相关信息	juicefs minio同步的commit	juicefs 1.3.0对应的minio是否同步	备注
CVE-2021-21287	在 SSRF 攻击中，攻击者利用服务器端功能读取或更新内部资源。攻击者可提供或修改一个 URL，使服务器端代码读取或提交数据；通过精心构造的 URL，攻击者可能读取服务器配置（如 AWS 元数据）、连接内部 HTTP 服务（如 HTTP 接口的数据库），或对未计划暴露的内部服务发起 POST 请求。	https://github.com/minio/minio/security/advisories/GHSA-m4qq-5f7c-693q issue； https://github.com/golang/vulndb/issues/2318 PR： https://github.com/minio/minio/pull/11337	https://github.com/juicedata/minio/commit/eb6871ecd960d570f7069887720 9e6db181bf276	已同步	

CVE-2021-43858	恶意客户端可以手工构造 HTTP API 调用，利用该字段更新用户策略，从而提升自身权限。	https://github.com/minio/minio/security/advisories/GHSA-j6jc-jqqc-p6cx issue： https://github.com/golang/vulndb/issues/285 PR： https://github.com/minio/minio/pull/7949	NA	未同步	
CVE-2021-21390	读取器在未验证的情况下就将数据返回给调用者，仅当遇到分块载荷末尾时才验证该分块的签名。	https://github.com/minio/minio/pull/11801	https://github.com/juicedata/minio/commit/e197800f9055489415b53cf137e31e194aaf7ba0	已同步	
CVE-2021-21362	missing user policy enforcement in PostPolicyHandler	https://github.com/minio/minio/pull/11682	https://github.com/juicedata/minio/commit/039f59b552319fcc2f83631bb421a7d4b82bc482	已同步	

CVE-2022-35919	拥有管理员权限的人可通过如下命令轻松读取任意操作系统路径的内容：mc admin update alias/ /etc/passwd	https://github.com/minio/minio/pull/15429	NA		juicefs已经禁用了update功能，因此没有影响?
CVE-2023-28434	利用精心构造的请求绕过元数据存储桶名称检查，在处理 `PostPolicyBucket`时将对象放入任何存储桶。	https://github.com/minio/minio/pull/16849	NA	未同步	
CVE-2023-25812	受影响的版本未能正确遵循BypassGoverance上的`Deny`策略。理想情况下，minio应该对所有尝试使用特殊头部`X-Amz-Bypass-Governance-Retention: true`删除 versionId 的用户返回"Access Denied"。然而，这一策略并未被遵循，请求将被允许，并且治理下的对象将被错误删除。	https://github.com/minio/minio/pull/16635	NA	未同步	
CVE-2023-27589	权限提升（Policy逃逸）	https://github.com/minio/minio/pull/16803	NA	未同步	

CVE-2023-28433	所有 Windows 用户都会受到影响。MinIO 未能过滤 `\` 字符，这允许跨任意对象放置。	https://github.com/minio/minio/security/advisories/GHSA-w23q-4hw3-2pp6 https://github.com/minio/minio/commit/8d6558b23649f613414c8527b58973fbdfa4d1b8 https://github.com/minio/minio/commit/b3c54ec81e0a06392abfb3a1ffcdc80c6fbf6ebc	NA	未同步	