预警编号：YJ-2018003

恒安嘉新

关于 Western Digital My Cloud NAS

设备存在高危漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 1 月 06 日

1 漏洞描述

近期，互联网爆出 6 起 Western Digital My Cloud NAS 设备高危漏洞，包括：Western Digital My Cloud NAS 设备信息泄露漏洞、Western Digital My Cloud NAS 设备拒绝服务漏洞、Western Digital My Cloud NAS 设备跨站请求伪造漏洞、Western Digital My Cloud NAS 设备命令注入漏洞、Western Digital My Cloud NAS 设备无限制文件上传漏洞、Western Digital My Cloud NAS 设备硬编码后门漏洞。综合利用上述漏洞，远程攻击者可发起拒绝服务器攻击、远程执行命令、获取 My Cloud 设备控制权。该漏洞危害程度为高危(High)。

2 影响范围

受影响的云端固件版本和型号如下：

My Cloud<=2.30.165

My Cloud Mirror <=2.30.165

受影响的设备型号：

My Cloud Gen 2

My Cloud PR2100

My Cloud PR4100

My Cloud EX2 Ultra

My Cloud EX2

My Cloud EX4

My Cloud EX2100

My Cloud EX4100

My Cloud DL2100

My Cloud DL4100

3 漏洞原理

Western Digital My Cloud NAS 是一款应用广泛的网络连接云存储设备，可用于托管文件，并自动备份和同步该文件与各种云和基于 Web 的服务。此外，该设备不仅可让用户共享家庭网络中的文件，而且私有云功能还允许用户随时随地访问该文件数据。

Western Digital My Cloud NAS 设备信息泄露漏洞 :攻击者可通过向 Web 服务器发送一个简单的请求来转储所有用户的列表，包括详细的用户信息，而不需要任何身份验证，如：GET /api/2.1/rest/users? HTTP/1.1

Western Digital My Cloud NAS 设备拒绝服务漏洞 : 该漏洞是由于未经身份验证的用户可为整个存储设备及其所有用户设置全局语言首选项所致 ,攻击者可能会恶意利用该功能导致 Web 界面拒绝服务。

Western Digital My Cloud NAS 设备跨站请求伪造漏洞 : 该漏洞是由于 WD My Cloud 网页界面中无有效地 XSRF 保护所致，攻击者可利用任何恶意网站使受害者的网络浏览器连接到网络上的 My Cloud 设备，诱使目标用户进行访问，获取 My Cloud 设备控制权。

Western Digital My Cloud NAS 设备命令注入漏洞 : 该注入漏洞可能与

跨站点请求伪造 XSRF 漏洞相结合 ,导致攻击者获得受影响设备的完全控制权(root 访问权限) 。

Western Digital My Cloud NAS 设备无限制文件上传漏洞 : 该漏洞是由于开发人员错误地实现了 gethostbyaddr() PHP 函数所致，漏洞存在于“multi_uploadify.php”脚本中。攻击者可使用参数 Filedata[0]将任意恶意文件上传到互联网易受攻击的存储设备所在的运行服务器，以 root 身份获得远程 shell。

Western Digital My Cloud NAS 设备硬编码后门漏洞:该漏洞是由于开发者将管理员用户名“mydlinkBRionyg”和密码“abc12345cba”，硬编码到二进制文件，且无法更改所致。攻击者可利用上述凭证登录到 WD My Cloud 设备，注入命令，导致 root shell。

4 修复建议

目前，厂商暂无详细的解决方案：

https://www.wdc.com/region-selector/splash-region.html