安全事件通告

西部数据 NAS 设备网络攻击通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	西部数据 NAS 设备网络攻击通告		
报告类型	安全事件通告	报告编号	
报告版本	1	报告日期	2021-06-28
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-06-28	360CERT	360CERT	撰写报告

目录

1 事件描述 3
2 风险等级 4
3 涉及漏洞 5
CVE-2018-18471: Axentra Hipserv XXE 漏洞 5
CVE-2018-18472：WD MyBook Live 远程命令执行漏洞 5
4 安全建议 6
5 相关空间测绘数据 7
6 时间线 8
7 参考链接 9
附录 10
A 产品侧解决方案 10
360 城市级网络安全监测服务 10
360 安全分析响应平台 10
360 本地安全大脑 11
360 终端安全管理系统 11

1 事件描述

2021 年 06 月 28 日，360CERT 监测发现WesternDigital发布了 RecommendedSecurityMeasuresforWDMyBookLiveandWDMyBookLiveDuo 的通告。西部数据已经确定，该公司的 My Book Live 设备遭到了攻击者的入侵，这种入侵会导致设备被恢复出厂设置，数据也被全部擦除。My Book Live 设备在 2015 年进行了最后的固件更新，目前已不再享受官方的系统升级支持。

对此，360CERT 建议 My Book Live 用户断开该设备与互联网的连接，以保护设备上的数据，并做好资产自查以及预防工作，以免遭受黑客攻击。事件等级：严重，事件评分：9.8。

2 风险等级

360CERT 对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

3 涉及漏洞

3.1 CVE-2018-18471: Axentra Hipserv XXE 漏洞

CVE: CVE-2018-18471

组件: Axentra Hipserv

漏洞类型: XXE

影响: 远程命令执行

简述: Axentra Hipserv 系统存在 XXE 漏洞，利用此漏洞的攻击者，可以在未授权的情况下，通过精心构造的恶意请求在设备上执行命令。

3.2 CVE-2018-18472 : WD MyBook Live 远程命令执行漏洞

CVE: CVE-2018-18472

组件: WD MyBook Live

漏洞类型: 命令执行

影响: 命令执行

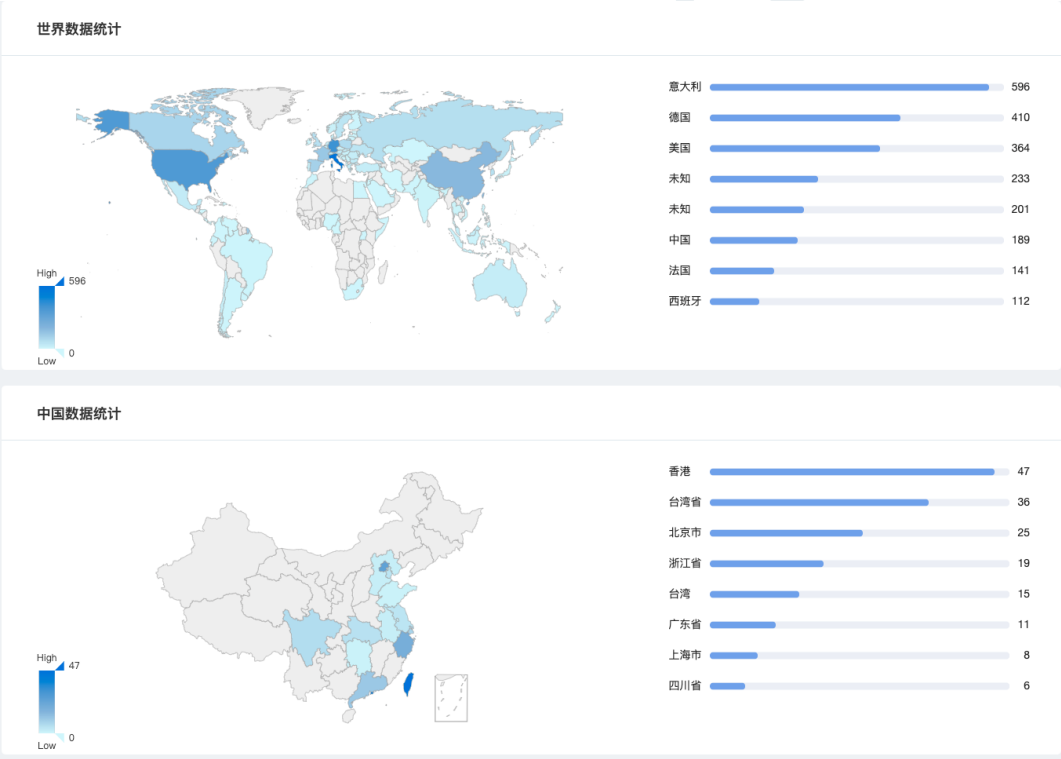
简述: 西部数据 WD MyBook Live 设备存在远程命令执行漏洞，利用此漏洞的攻击者，可以在未授权的情况下，通过精心构造的恶意请求在设备上执行命令。

4 安全建议

1. My Book Live 用户断开 WD MyBook Live 设备与互联网的连接，以保护设备上的数据。
2. 在必须联网的情况下，建议使用 VPN 来保护计算机和设备免受黑客入侵。

5 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现WDMyBookLive具体分布如下图所示。



6 时间线

2021-06-25 Western Digital 发布报告

2021-06-28 360CERT 发布预警报告

7 参考链接

https://www.westerndigital.com/support/productsecurity/wdc-21008-recommended-security-measures-wd-mybooklive-wd-mybookliveduo

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。

A.2 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或 (shaoyulong#360.cn) 获取对应产品。

A.3 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.4 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全

产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。