

安全漏洞通告

【POC 公开】 CVE-2021-31166: Windows HTTP 协议远程
代码执行漏洞通告

360CERT

北京奇虎科技有限公司 | 2021-05-18

报告信息

报告名称	【POC 公开】 CVE-2021-31166: Windows HTTP 协议远程代码 执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-051702
报告版本	1	报告日期	2021-05-18
报告作者	360CERT	联系方式	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-05-18	360CERT	360CERT	撰写报告

目录

一、	漏洞档案	1
二、	漏洞简述	2
三、	漏洞评级	3
四、	漏洞详情	4
五、	影响版本	6
六、	漏洞列表	7
七、	安全建议	8
	(一) 通用修补方案	8
	(二) 临时修补方案	8
八、	产品侧解决方案	9
	(一) 360 安全卫士	9
	(二) 360AISA 全流量威胁分析系统	9
	(三) 360 本地安全大脑	10
九、	参考链接	11
附录 A	报告风险等级说明	12
附录 B	影响面说明	14
附录 C	360 内部评分体系	15

一、 漏洞档案



漏洞类型	代码执行
CVE 编号	CVE-2021-31166
相关厂商	microsoft
相关组件	windows server 等
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-05-17
报告生成时间	2021-05-18

二、漏洞简述

2021年05月17日，360CERT监测发现国外安全研究员发布了 Windows HTTP 协议远程代码执行漏洞的 POC 详情，漏洞编号为 CVE-2021-31166，漏洞等级：严重，漏洞评分：9.8。

该漏洞在微软 5 月补丁日中完成了修复，微软官方将其标记为可造成蠕虫攻击及易被攻击，攻击者可以利用该漏洞造成大范围蠕虫攻击。

对此，360CERT 建议广大用户及时将 Windows 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、漏洞详情

CVE-2021-31166: HTTP 协议远程代码执行漏洞

CVE: CVE-2021-31166

组件: HTTP Protocol

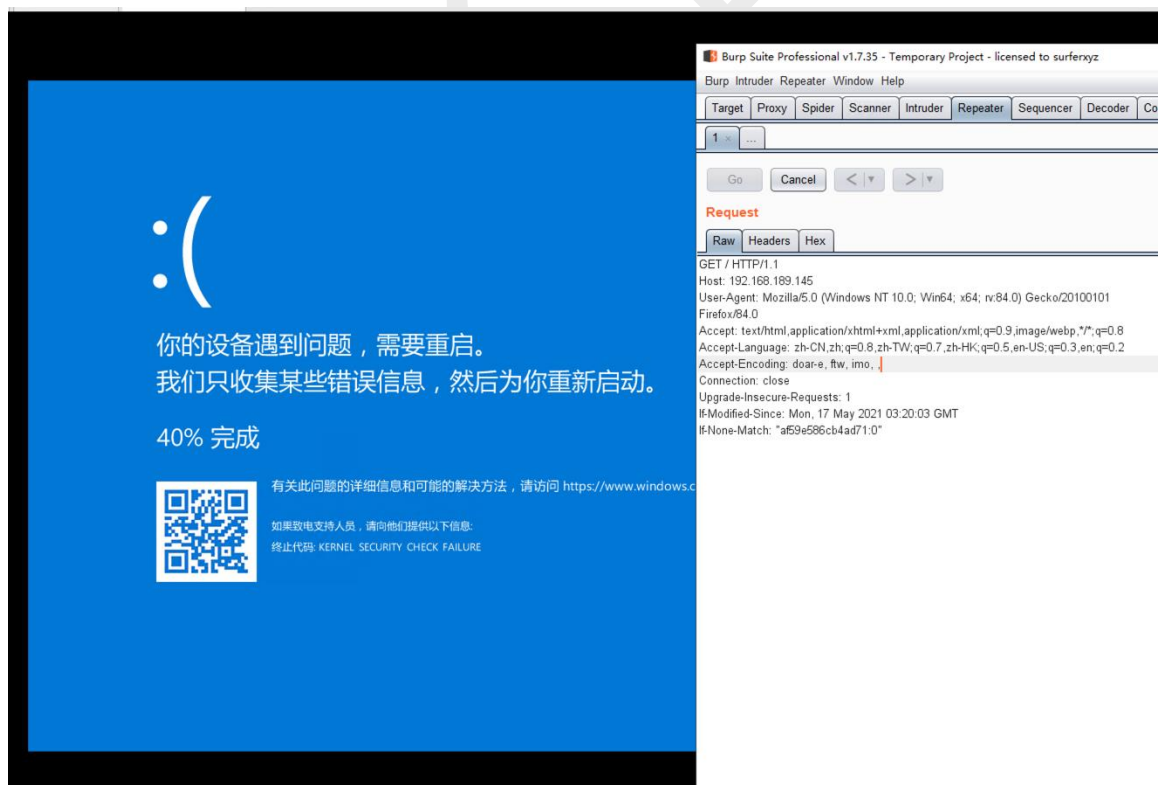
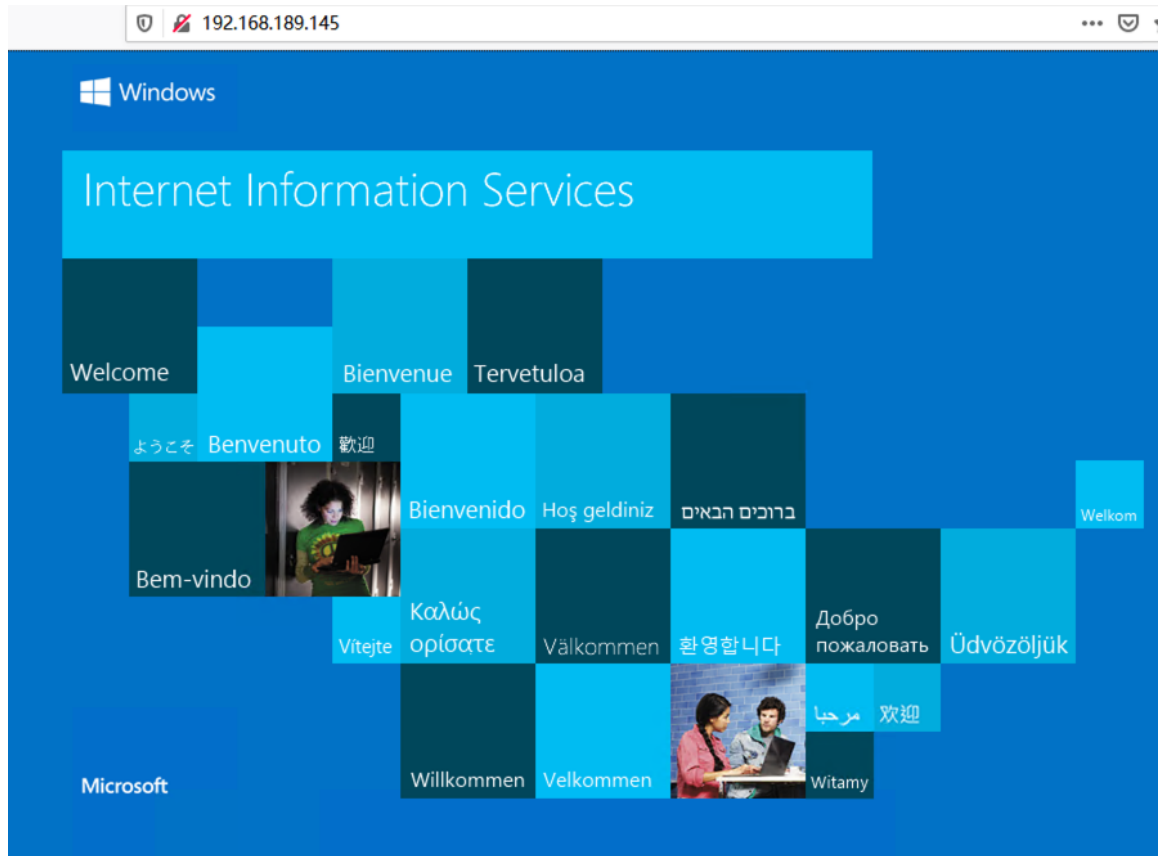
漏洞类型: 代码执行

影响: 服务器接管

简述: 漏洞存在于 Windows 10 和 Windows Server 中的 HTTP 协议栈(http.sys)处理程序中, 该程序广泛的用于应用之间或设别之间的通信中。常见的组件如 Internet Information Services (IIS) 便使用该程序进行通信处理。

未授权的攻击者可以构造恶意请求包攻击目标服务器, 成功利用该漏洞的攻击者可以在目标服务器执行任意代码。

目前该漏洞 360CERT 已完成 poc 编写和利用复现:



五、影响版本

产品名称	影响版本
Microsoft:Windows	2004,20H2
Microsoft:Windows Server	Version 2004

360CERT

六、漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-31166	代码执行	服务器接管	严重

360CERT

七、安全建议

(一) 通用修补方案

360CERT 建议通过安装 360 安全卫士进行一键更新。

应及时进行 Microsoft Windows 版本更新并且保持 Windows 自动更新开启。

Windows server / Windows 检测并开启 Windows 自动更新流程如下：

- 点击开始菜单，在弹出的菜单中选择“控制面板”进行下一步。
- 点击控制面板页面中的“系统和安全”，进入设置。
- 在弹出的新的界面中选择“windows update”中的“启用或禁用自动更新”。
- 然后进入设置窗口，展开下拉菜单项，选择其中的自动安装更新（推荐）。

(二) 临时修补方案

通过如下链接寻找符合操作系统版本的漏洞补丁，并进行补丁下载安装。

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166>

八、产品侧解决方案

(一) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。



(二) 360AISA 全流量威胁分析系统

针对微软本次安全更新，360AISA 已基于流量侧提供对应检测能力更新，请 AISA 用户联系 techsupport@360.cn 获取更新，尽快升级检测引擎和规则，做好安全防护工作。



(三) 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。



九、 参考链接

1. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166>

2. <https://github.com/0vercl0k/CVE-2021-31166>

<https://github.com/0vercl0k/CVE-2021-31166>

360CERT

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	<ol style="list-style-type: none"> 1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	<ol style="list-style-type: none"> 1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	<ol style="list-style-type: none"> 1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	<ol style="list-style-type: none"> 1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	<ol style="list-style-type: none"> 1. $4.0 \leq 360\text{CERT 评分} < 7$ 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 <ol style="list-style-type: none"> a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	<ol style="list-style-type: none"> 1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	<ol style="list-style-type: none"> 1. $0 \leq 360\text{CERT 评分} < 4$ 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在“CVSS 漏洞评分体系”的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 - 10.0	严重
7.0 - 8.9	高危
4.0 - 6.9	中危
0 - 3.9	低危