



# 网络安全预警通报

2026 年第 6 期（总第 64 期）

西安交通大学网络信息中心 2026 年 07 月 16 日

---

【预警类型】高危预警

【预警内容】

## Microsoft Windows HTTP.sys 远程代码执行漏洞（CVE-2026-47291）高危风险通报

### 一、漏洞概述

近期，微软官方披露了 Windows HTTP 协议栈（HTTP.sys）中的一个高危远程代码执行漏洞（CVE-2026-47291）。HTTP.sys 是 Windows 内核模式 HTTP 驱动程序，负责解析系统接收的 HTTP/HTTPS 请求，广泛应用于 IIS、WinRM 及基于 Windows HTTP Server API 开发的各类应用程序。

该漏洞源于 HTTP.sys 在处理特定 HTTP 请求头字段时存在整数溢出缺陷，导致后续缓冲区分配异常，并最终引发内核堆缓冲区溢出。未经身份验证的远程攻击者可向目标系统发送特制 HTTP 请求，在无

需用户交互的情况下触发漏洞，最终实现远程代码执行并获得 SYSTEM 权限。

微软已将该漏洞评估为 “Exploitation More Likely（更可能被利用）”，漏洞 PoC 已于 2026 年 7 月公开，预计后续将出现自动化扫描及攻击工具，建议各单位立即开展受影响资产排查并及时完成安全加固。

## 二、漏洞详情

### 1.技术原理

漏洞编号 CVE-2026-47291

漏洞名称 Windows HTTP.sys 远程代码执行漏洞

漏洞类型 远程代码执行（RCE）

漏洞等级 严重（Critical）

公布日期 2026 年 6 月 9 日

PoC 公开时间 2026 年 7 月 11 日

CVSS 3.1 评分 9.8

产生原因：

HTTP.sys 在解析 HTTP 请求过程中，对 Content-Length、Transfer-Encoding 等 HTTP 头字段进行长度计算时，存在整数溢出（Integer Overflow）缺陷。当攻击者构造异常长度值时，可导致缓冲区大小计算错误，使系统分配小于实际需求的内核缓冲区。

随后 HTTP.sys 继续向该缓冲区写入完整请求数据，引发内核堆缓冲区溢出（Heap Buffer Overflow），攻击者可进一步破坏内核对象、劫持程

序执行流程，最终在 Windows 内核态执行任意代码，并获取 SYSTEM 最高权限。

由于漏洞发生于 HTTP 请求解析阶段，在身份认证之前即可触发，因此无需登录系统、无需用户交互，仅需目标开放 HTTP 相关服务即可实施攻击。

## 2.利用条件

- 攻击者无需获得目标系统任何账户权限；
- 目标 Windows 系统启用了 HTTP.sys 服务，并开放 HTTP/HTTPS 相关监听端口（如 80、443、5985、5986 等）；
- 目标系统版本受该漏洞影响且尚未安装微软官方安全补丁；
- 攻击者能够与目标建立网络连接，并发送特制 HTTP 请求即可完成漏洞触发。

## 三、漏洞影响范围

### 1.受影响版本

目前确认受影响的 Windows 系统包括但不限于：

Windows 10 (1607、1809、21H2、22H2)

Windows 11 (23H2、24H2、25H2、26H1)

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

## Windows Server 2025

以及使用 HTTP.sys 组件提供 HTTP 服务的相关 Windows 版本。

### 2.威胁严重性

该漏洞属于无需认证即可远程利用的高危远程代码执行漏洞，攻击复杂度低，不依赖用户交互，CVSS 评分高达 9.8。

攻击成功后，攻击者可直接获得 SYSTEM 权限，并进一步实施以下攻击行为：

- 在目标主机部署后门程序或 Rootkit，实现长期持久化控制；
- 窃取 LSASS 进程中的系统凭据及域账户信息，开展横向移动攻击；
- 绕过或关闭终端安全防护软件（EDR、杀毒软件等）；
- 部署勒索软件，加密服务器及业务数据；
- 完全控制受影响服务器，对业务系统造成严重影响。

由于漏洞发生在内核 HTTP 协议解析阶段，攻击过程产生的应用层日志较少，攻击行为具有较强隐蔽性，一旦互联网暴露相关服务，极易成为自动化攻击目标。

## 四、处置建议

### 1.官方修复方案

微软已于 2026 年 6 月安全更新中发布针对 CVE-2026-47291 漏洞的安全补丁，建议立即通过 Windows Update 或微软官方安全更新渠道完成补丁升级，优先修复互联网暴露资产、IIS 服务器及启用 WinRM 服务的主机。

参考链接：<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47291>

## 2.临时缓解措施（建议根据自身业务情况实施）

在无法第一时间完成补丁升级的情况下，可采取以下临时缓解措施：

限制 80、443、5985、5986 等 HTTP 相关端口，仅允许可信 IP 访问，减少互联网暴露面；

关闭不必要的 HTTP 服务及 WinRM 服务，降低漏洞攻击面；

在边界防火墙、WAF 或 IPS 设备中部署针对异常 HTTP 请求的检测与拦截规则；

加强互联网暴露 Windows 服务器的访问监测，及时发现异常 HTTP 请求及攻击行为。

建议同时持续关注微软官方安全公告，及时获取后续补丁更新及安全建议。