网络安全预警通报

2026 年第 13 期（总第 71 期）

西安交通大学网络信息中心 2026 年 11 月 26 日

【预警类型】严重预警

【预警内容】

NGINX 堆缓冲区溢出高危漏洞安全预警通报

一、病毒概述

近日，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）监测发现，NGINX 存在堆缓冲区溢出高危漏洞。NGINX 是广泛应用于 Web 服务部署、负载均衡及邮件代理等场景的开源软件。

该漏洞源于 NGINX 处理 HTTP/2 协议流量控制窗口时存在设计缺陷。攻击者可向启用 HTTP/2 协议的服务器发送特制网络流量，触发堆缓冲区溢出，可能导致服务崩溃、内存破坏，甚至远程代码执行。

该漏洞具有以下特点：

（1）危害严重：可能造成服务器内存破坏、服务中断，甚至远程代码执行。

（2）影响范围广：涉及 NGINX 开源版、NGINX Plus 及部分内嵌 NGINX 核心组件的产品。

（3）攻击门槛较低：攻击者可通过向启用 HTTP/2 的服务器发送特制流量发起攻击。

二、病毒详情

1.技术原理

该漏洞存在于 NGINX 处理 HTTP/2 协议流量控制窗口的过程中，由相关处理逻辑设计缺陷导致堆缓冲区溢出。攻击者通过构造特制 HTTP/2 请求流量，可能触发内存异常写入，造成堆内存破坏，进一步引发服务崩溃或远程代码执行。

2.涉及病毒详情

漏洞名称：NGINX 堆缓冲区溢出高危漏洞

漏洞类型：堆缓冲区溢出

影响组件：NGINX HTTP/2 处理模块

威胁等级：高危

攻击方式：发送特制 HTTP/2 网络流量

主要危害：服务崩溃、内存破坏、远程代码执行。

主要受影响版本：

（1）NGINX 开源版：1.9.5 至 1.30.6、1.31.0 至 1.31.8。

（2）NGINX Plus：37.0.0 至 37.0.7.1、37.1.0 至 37.2.0.1、R34 至 R36。

（3）部分内嵌 NGINX 核心组件的产品，包括 NGINX Instance Manager、NGINX Ingress Controller 等。

3、主要识别特征

根据公开披露的信息，发现以下情况时应提高警惕：

（1）服务器部署 NGINX 开源版或 NGINX Plus。

（2）NGINX 版本处于上述受影响范围。

（3）服务器启用了 HTTP/2 协议。

（4）使用 NGINX Ingress Controller 等内嵌 NGINX 核心组件的产品。

三、漏洞影响范围

1. 影响范围

该漏洞主要影响使用受影响版本 NGINX 且启用 HTTP/2 协议的服务器，涉及 Web 服务、反向代理、负载均衡及容器化部署环境。相关单位应重点排查对公网开放的 NGINX 服务及相关组件。

2. 威胁严重性

攻击者利用该漏洞可能造成服务器堆内存破坏、业务服务异常中断，严重情况下可能实现远程代码执行，进而导致服务器被控制及业务数据泄露，存在较高安全风险。

四、处置建议

1. 开展资产排查。全面梳理 NGINX 服务器及相关组件，重点核查版本信息、HTTP/2 协议启用情况及公网暴露情况。

2. 及时升级修复。将受影响版本升级至已修复的安全版本，消除漏洞风险。

3. 加强访问控制。对公网开放的 NGINX 服务加强访问控制，非必要情况下限制 HTTP/2 协议访问。

4. 加强安全监测。关注异常 HTTP/2 请求、服务异常崩溃及可疑网络流量，发现疑似攻击行为及时开展排查和应急处置。