赣州市网络与信息安全信息通报中心

赣市通报[2025] 19号

警惕境外产品网络安全漏洞

市有关单位:

工作发现，思科、Anysphere公司产品存在高危安全漏洞：一是思科身份服务引擎等设备存在多个远程代码执行漏洞（NVDB-CNVDB-2025459499/CVE-2025-20281、NVDB-CNVDB-2025187815/CVE-2025-20282、NVDB-CNVDB-2025886020/CVE-2025-20337），攻击者可利用其执行任意命令。二是Anysphere公司Cursor代码编辑器存在远程代码执行漏洞（NVDB-CNVDB-2025549164/CVE-2025-54135），攻击者可利用其执行任意代码。

请各单位高度重视，组织本行业、本单位做好以下工作：一是全面排查相关产品使用情况，压实网络运营者网络安全主体责任，切实做好网络安全防护。二是针对性加强网络安全保护和技术措施，及时堵塞漏洞，消除风险隐患。三是持续做好网络安全监测和应急处置，发现遭网络攻击情况要第一时间妥善处置并报告我中心。

各单位接此通知后，及时抓好各项工作措施落实，对未履行网络安全义务造成严重后果的，将依规问责。

联系人：邹锋、梁薇　　联系电话：0797-8685893

附件：漏洞详情

赣州市网络与信息安全信息通报中心

2025年9月9日

报：声宏同志，省网络与信息安全信息通报中心。

送：各有关单位、各县（市、区）公安局（分局）网络安全保卫大队

审批：张　勇　　核稿：熊海欣　　编校：梁　薇

附件

漏洞详情

一、思科身份服务引擎等设备远程代码执行漏洞（NVDB-CNVDB-2025459499/CVE-2025-20281、NVDB-CNVDB-2025187815/CVE-2025-20282、NVDB-CNVDB-2025886020/CVE-2025-20337）

思科身份服务器引擎（Cisco ISE）和被动身份连接器（Cisco ISE-PIC）是思科公司开发的网络访问控制解决方案，用于网络访问控制与安全管理。由于其 API 中存在多个漏洞，可被未经身份验证的攻击者利用，远程执行恶意代码，获取系统最高 root 权限。

目前思科公司已修复该漏洞并发布安全公告。建议尽快升级消除风险隐患。

影响版本:

3.3≤ver<3.3 patch7、3.4≤ver<3.4 patch2

二、Anysphere 公司 Cursor 代码编辑器远程代码执行漏洞（NVDB-CNVDB-2025549164/CVE-2025-54135）

Cursor 是美国 Anysphere 公司开发的一款人工智能驱动的代码编辑器。由于其新建 MCP 配置文件时无需询问用户，攻击者可采取间接提示词注入的攻击方式将恶意指令写入配置文件，进而实现远程代码执行。

目前 Cursor 官方已修复该漏洞并发布安全版本，建议尽快升级至最高版本。

影响版本:

Cursor<1.3.9