Ivanti 多款产品缓冲区溢出漏洞(CVE-2025-0282)

■ **通告编号**	**NS-2025-0001**	■ 发布日期	**2025-01-10**
■ **漏洞危害**	**攻击者利用此漏洞，可实现任意代码执行。**		
■ **TAG**	Ivanti、缓冲区溢出、CVE-2025-0282		

一. 漏洞概述

近日，绿盟科技监测到 Ivanti 发布安全公告，修复了 Ivanti 多款产品缓冲区溢出漏洞(CVE-2025-0282)。由于 Ivanti Connect Secure、Ivanti Policy Secure 和 Ivanti Neurons for ZTA 网关中存在基于堆栈的缓冲区溢出，未经身份验证的攻击者可通过发送特制的数据包触发缓冲区溢出，从而实现在目标系统上执行任意代码。CVSS 评分 9.0，目前已发现在野利用，请相关用户尽快采取措施进行防护。

Ivanti Connect Secure（ICS）是一种 SSL VPN 解决方案，它允许远程和移动用户从任何支持网络的设备访问公司资源；Ivanti Policy Secure（IPS）是一种网络访问控制 (NAC) 解决方案，可为授权和安全的用户和设备提供访问权限；Ivanti Neurons for ZTA 是一种 SaaS 交付的零信任网络访问解决方案，可为组织的应用程序基础设施提供完全托管的零信任身份验证和访问控制。

参考链接：

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

二. 影响范围

受影响版本

- 22.7R2 <= Ivanti Connect Secure <= 22.7R2.4
- 22.7R1 <= Ivanti Policy Secure <= 22.7R1.2
- 22.7R2 <= Ivanti Neurons for ZTA <= 22.7R2.3

不受影响版本

- Ivanti Connect Secure >= 22.7R2.5
- Ivanti Policy Secure > 22.7R1.2（1 月 21 日发布）
- Ivanti Neurons for ZTA gateways >= 22.7R2.5（1 月 21 日发布）

三. 漏洞防护

3.1 官方升级

目前官方已发布新版本修复了该漏洞，请受影响的用户尽快升级版本进行防护，下载链接：https://portal.ivanti.com/

注：使用 Ivanti Connect Secure 的用户，Ivanti 官方建议在升级到 22.7R2.5 版本之前，可对 ICT 扫描无异常的设备进行出厂重置；若 ICT 结果显示存在入侵迹象，需将设备恢复出厂设置以确保删除所有恶意软件，然后使用 22.7R2.5 版本将设备重新投入生产。

参考链接：https://forums.ivanti.com/s/article/Recovery-Steps

声明