Comware V7防火墙是否涉及Citrix Bleed漏洞(CVE-2023-4966)

漏洞相关 **孔凡安** 2023-11-14 发表

问题描述

防火墙是否涉及Citrix Bleed漏洞(CVE-2023-4966)

Citrix Bleed漏洞(CVE-2023-4966)排查和整改指南

一、漏洞介绍

Citrix NetScaler Gateway和Citrix Systems NetScaler ADC是美国思杰系统（Citrix Systems）公司的产品，主要用于企业网络的构建和管理。NetScaler Gateway提供安全的远程访问功能，为企业网络外部的用户提供对内部网络的安全访问。同时，它还可以与NetScaler ADC集成，利用其负载平衡功能来提高网络性能。Citrix Systems NetScaler ADC则是一款应用程序交付控制器，可以加速、保护和优化应用程序的交付。

二、漏洞危害

1.该漏洞存在于Citrix NetScaler ADC 和 Gateway 设备中，是一个信息泄露漏洞。要利用该漏洞，需要将设备配置为网关（VPN 虚拟服务器、ICA 代理、CVPN、RDP 代理）或授权和计费 (AAA) 虚拟服务器。未授权的远程攻击者可通过利用此漏洞，窃取敏感信息。

2.通过利用该漏洞，攻击者可以获得对 NetScaler ADC 和网关设备的内存访问权限，这使他们能够提取会话 COOKIE 并尝试绕过身份验证。这意味着即使打了补丁的实例也面临被利用的风险，因为会话令牌保留在内存中。

三、漏洞等级

该漏洞影响面广泛，攻击价值高，且利用难度低，故漏洞威胁等级为严重级别。

四、影响版本

组件	影响版本	安全版本
Citrix:NetScaler ADC 和 NetScaler Gateway	14.1 < 14.1-8.50	>= 14.1-8.50
Citrix:NetScaler ADC 和 NetScaler Gateway	13.1 < 13.1-49.15	13.1 >= 13.1-49.15
Citrix:NetScaler ADC 和 NetScaler Gateway	13.0 < 13.0-92.19	13.0 >= 13.0-92.19
Citrix:NetScaler ADC 13.1-FIPS	< 13.1-37.164	>= 13.1-37.164
Citrix:NetScaler ADC 12.1-FIPS	< 12.1-55.300	>= 12.1-55.300
Citrix:NetScaler ADC 12.1-NDcPP	< 12.1-55.300	>= 12.1-55.300

五、修复建议

根据影响版本中的信息，排查并升级到安全版本，或直接访问参考链接获取官方更新指南。

参考链接

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

集团SOC漏洞治理团队

2023年11月13日

解决方法

不涉及，未使用该组件。