HDM扫描出ICMP时间戳检测漏洞规避方案

HDM 金占勇 2024-11-20 发表

组网及说明

客户使用扫描软件检测出HDM版本存在ICMP时间戳检测的低危漏洞

告警信息

漏洞描述：

远程主机响应ICMP时间戳请求。 时间戳回复是回复时间戳消息的ICMP消息。 它由时间戳的发送者发送的始发时间戳以及接收时间戳和发送时间戳组成。 这个信息理论上可以用来开发其他服务中基于时间的弱随机数发生器。风险级别低。

问题描述

1.我司对于此安全漏洞的处理策略是

NA	ICMP_timestamp请求响应漏洞	内部测试	HDM 1.*.*通用维护及大客户所有版本 HDM 2.*.* 和3.*所有版本	HDM 所有版本评估不解决挂起	202107300854	挂起	分析影响，加影响较小，挂起

漏洞描述：

远程主机响应ICMP时间戳请求。 时间戳回复是回复时间戳消息的ICMP消息。 它由时间戳的发送者发送的始发时间戳以及接收时间戳和发送时间戳组成。 这个信息理论上可以用来开发其他服务中基于时间的弱随机数发生器。风险级别低。

过程分析

规避措施：

ICMP timestamp请求和响应本身不是直接的“漏洞”，但它可能会在某些情况下被滥用。适当的网络配置和安全措施可以有效缓解这些风险：

1.防火墙上过滤外来(INPUT)的ICMP timestamp（类型13）报文以及外出(OUTPUT)的ICMP timestamp回复报文。

综上所述，建议此漏洞无需修复。该漏洞风险级别低且可在客户端配置防火墙来规避。

解决方法

对于配置防火墙有2种方案，一种是客户端的防火墙设置

还有一种是机台本身的防火墙配置iptableds

禁用方式：

通过SOL进入到BMC后台，发送如下命令

```
iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP
iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROP

ip6tables -A INPUT -p icmpv6 --icmpv6-type 136 -j DROP
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type 137 -j DROP
```