2016 年 4 月 27 日，星期三

漏洞聚焦：NTPD 漏洞最新动态

作为 Linux 基金会核心基础设施计划 (CII) 的参与者之一，思科在评估网络时间协议守护进程 (NTPD) 的安全缺陷方面为 CII 做出了巨大贡献。以前，我们曾在 NTPD 中发现了一系列漏洞。随着研究不断进行，我们又在该软件中发现了更多的漏洞。

从 2013 年起，犯罪者便开始滥用 NTP 数据包来放大拒绝服务攻击。NTPD 之所以对攻击者有吸引力，一是因为该软件的使用十分普遍，二是因为协调时间对于确保许多服务正常运行极为重要。NTPD 漏洞可以使攻击者冒充 NTPD 指令修改时间，将时间设置为任意值。这样一来，攻击者就能阻止时间依赖型服务启动（因为永远无法达到激活时间），进而达到以下目的：使系统重复达到服务激活时间，致使系统资源耗尽；利用过期认证获得系统访问权限；使合法的服务和缓存过期，造成拒绝服务。因此，发现并修复时间服务中存在的漏洞是一项非常重要的工作。

思科在 NTPD 中发现了 6 个新漏洞。攻击者可以利用这些漏洞制作 UDP 数据包，从而为拒绝服务创造条件，或者阻止系统设置正确的时间。我们建议所有用户升级到 NTPD 的最新版本。

CVE-2016-1550 NTP 身份验证潜在计时漏洞

发现者：Matthew Van Gundy 和 Stephen Gray（思科高级安全计划团队）。

根据 RFC5905 中的描述，NTP 数据包可以包含一个密钥 ID。该密钥 ID 是一个 32 位无符号整数，用于指定在相互协调时间的系统之间共享的 128 位密钥。此密钥用于计算该数据包的 MD5 消息摘要值，用于接收方验证发送方身份。

如果数据包的摘要值与客户端使用密钥计算出的值不匹配，该数据包将被拒绝。接收方随即会向发送方发出一个加密 NAK 数据包，以通知摘要值不正确。但是，观察者可以利用发送此加密 NAK 数据包的计时来获知发生摘要值不匹配的位置。因首字节不匹配而生成加密 NAK 数据包的时间，要比因后面的字节不匹配而生成加密 NAK 数据包的时间要短。攻击者可以通过暴力破解 MD5 摘要值并检查返回的加密 NAK 数据包的计时来获取共享密钥的值。一旦取得密钥值，攻击者便可以发送伪造的 NTP 数据包，成功通过接收方的身份验证。

已确认存在此漏洞的版本：
NTP 4.2.8p4，NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92
此漏洞可被用于传播病毒。

CVE-2016-1551 NTP Refclock 模拟漏洞

发现者：Matt Street（思科高级安全计划团队）和其他协力者。

NTPD 绝对信任由 127.127.0.0/16 范围内的 IP 地址发起的参考时钟 NTP 流量。这意味着利用 127.127.0.0/16 范围内的 IP 地址成功发送伪造 NTP 数据包的攻击者，会被配置了参考时钟的系统视为可靠来源而加以信任。

根据 RFC1918，IP 地址范围 127.0.0.0/8 是私有地址，由这些地址发起的流量不应传递到 NTPD，而是应该被操作系统或路由器过滤掉。如果攻击者成功送出伪造的数据包，使目标系统将其视为受信任的对等点，他们就能利用这种信任关系篡改目标系统的时间。

在实际中，此类数据包会被大多数现代操作系统拒绝，所以不会传递到 NTPD。如果操作系统不会自动拒绝此类数据包，可以通过部署防火墙来丢弃从该地址范围发起的任何数据包。除非十分必要，否则不建议将守护进程配置为侦听 127.0.0.0/8 范围内的地址，以免因为此漏洞和其他类似漏洞而受到侵害。

已确认存在此漏洞的版本：
NTP 4.2.8p3，NTPsec a5fb34b9cc89b92a8fef2f459004865c93bb7f92
此漏洞可被用于传播病毒。

CVE-2016-1549 NTP 短暂关联 Sybil 漏洞

发现者：Matthew Van Gundy（思科高级安全计划团队）。

NTP 协议允许系统之间通过建立对等关联来计算公共系统时间，以代替通过客户端-服务器关系来套用参考时钟指定的权威时间值。这种对等关系在性质上是临时的，而且随时都能建立。客户端会毫无保留地认为，在建立对等关系之前，所要连接的对等点已使用前文介绍的密钥机制进行了身份验证。

但是，可以共享相同密钥的对等点数量是没有限制的。如果攻击者发现了某个密钥的标识（例如利用 CVE-2016-1550 中描述的机制），该密钥就有可能被用于创建大量恶意对等点。通过利用这些恶意对等点向客户端播发相同的错误时间，攻击者就能强制客户端像接受正确时间一样接受错误的时间。事实上，大量恶意对等点能够掩盖非恶意对等点共享的正确时间值。

已确认存在此漏洞的版本：
NTP 4.2.8p3，NTP 4.2.8p4，NTPsec 3e160db8dc248a0bcb053b56a80167dc742d2b74，NTPsec a5fb34b9cc89b92a8fef2f459004865c93bb7f92
此漏洞可被用于传播病毒。

CVE-2016-1547 可抢占式关联解除漏洞

发现者：Stephen Gray 和 Matthew Van Gundy（思科高级安全计划团队）。

在特定情况下，通过发送伪造的数据包来通知接收方它们的请求未成功通过身份验证，可以中断对等 NTPD 系统之间的关联。身份验证失败时发送的加密 NAK 数据包本身是未经过身份验证的。故此，攻击者可以伪造源于合法对等点的加密 NAK 数据包发送给接收方，强制发送方中断关联。通过重复发送伪造的加密 NAK 数据包，攻击者可以阻止对等点重新建立对等关系，从而造成拒绝服务。

已确认存在此漏洞的版本：
NTP 4.2.8p3，NTP 4.2.8p4，NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92
此漏洞可被用于传播病毒。

CVE-2016-1548 Xleave 透视：NTP 基本模式到交错模式

发现者：Jonathan Gardner（思科高级安全计划团队）和 Miroslav Lichvar (RedHat)，二人分别独立发现。

NTP 规范支持交错模式，允许一个数据包中包含标记前一个数据包的发送时间的时间戳。这是为了更准确地计算发送前处理数据包所需的时间。

攻击者可以通过发送经过特殊设计的数据包，强制 NTPD 客户端从基本客户端-服务器模式切换到交错模式，即使客户端未配置为采用交错模式也是如此。模式切换成功后，客户端将会

拒绝由之前关联的服务器发出的任何后续数据包，而攻击者却能够发送后续数据包，将客户端上的时间设置为攻击者选择的值。

此漏洞是由 NTPD 检查传入数据包的机制导致的。在基本模式下，客户端在收到请求数据包时发送的响应数据包中会包含原始时间戳，原始时间戳会被设置为与请求的传输时间戳相同。如果不符合这种情况，NTPD 会检查数据包是否为交错模式数据包，再决定是否将其丢弃。如果原始时间戳与目的时间戳（即客户端收到对等点发出的数据包的最后时间）相同，客户端便会被设置为交错模式。要利用这个漏洞，攻击者必须知道目的时间戳的值。此值可以通过许多方式获取，包括：使用 NTPD 查询工具得到；根据响应数据包的数据推导得出；或者通过暴力破解获得。

已确认存在此漏洞的版本：
NTP 4.2.8p4，NTPSec aa48d001683e5b791a743ec9c575aaf7d867a2b0c
此漏洞可被用于传播病毒。

结论

NTPD 守护进程是许多系统的重要组成部分，可确保系统时钟与公共标准进行同步。思科致力于确保这些基本而重要的系统组件尽可能没有漏洞。为此，思科的漏洞研究团队本着负责的精神，在与相关实体共同得出修复方案后在此披露以上漏洞。我们建议系统管理员尽快安装相关补丁或升级 NTPD 版本。

缓解措施

产品	保护
AMP	不适用
CWS	不适用
ESA	不适用
网络安全	✔
WSA	不适用

为了保护我们的客户，Talos 已经发布了相关规则来检测利用这些漏洞的攻击尝试。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心、FireSIGHT 管理中心或 Snort.org。

Snort 规则：36536、37841-37843。

时间表

2016 年 2 月 11 日：厂商漏洞发布
2016 年 4 月 26 日：漏洞修补完毕
2016 年 4 月 26 日：正式公开发布

发布者：MARTIN LEE；发布时间：上午 10:07

标签：CVE-2016-1547、CVE-2016-1548、CVE-2016-1549、CVE-2016-1550、CVE-2016-1551、NTPD、漏洞聚焦