Cisco IOS Router Exploitation

APR 22ND, 2016

论文下载

Available Vulnerabilities

- 2008 年Cisco Systems’ Product Security Advisory公开了14个漏洞，基本上所有的描述都是造成DoS
- 有理由相信不是memory corruption而是 insufficient handling of exceptional states
- Service Vulnerabilities
    - 防火墙，导致现在(2009年)攻击开始从server向client转移
    - Cisco IOS里有HTTP(S), FTP, TFTP, SSH, TELNET, 但是”For attackers seeking to gain control of important network infrastructure, such services are not of interest, as well-managed networks will not make use of such services on their core routing infrastructure.”
    - 网络设备中会使用的协议EIGRP, OSPF, ISIS, BGP
        - BGP: the service will not be visible as such to any remote network node
        - Other routing specific services, such as OSPF and EIGRP, require the network traffic to be received on an IPv4 multicast address, effectively making sure that the sender is

        within the same multicast domain as the receiving router.
        - 但是Cisco IOS IP options vulnerability是一个例外
        - 其他今年加入到IOS的服务包括VoIP， SSL VPN， 包过滤Web Service Management Agent(SOAP),XML-PI和H.323
- Client Side Vulnerabilities：But up until now, client side vulnerabilities have not played any role in Cisco IOS attacks.
- Transit Vulnerabilities
    - triggered by traffic passing through the router
    - Transit Vulnerabilities are extremely rare.
        - 原因在于包转发通过fast-path转发，所以除了第一个包之外，其他的处理过程都通过硬件来做了。。
        - 还有一些包会被”punted”, 从硬件退回给CPU来处理，作者提了两个可能：（1）目的IP是Router自己，但是这就不再是一个Transit Vul了；（2）IP fragment reassembly
    - So far, no true Transit Vulnerability is known to the author.

Architectural Issues

- 由于不知道系统架构，所以exp很难写。。
- 平坦的内存，进程共享内存，共享同一个堆。
- IOS uses a run-to-completion scheduling for its processes. All processes that receive execution must return to the scheduler in due time, in order to allow the execution of other processes.

- 与并没有windows异常处理机制可以使用，所有的异常都会导致系统直接重启(应该是在比较SEH什么的吧。。)
- 并不是用user land隔离内核，所有代码都在privilege level上。
- 每个进程的Stack只有6000Byte。。。溢出数据过多就会覆盖到更靠前的heap header.

The Return Address

- Return into Known Code
    - 任何代码重用的攻击都要知道代码的地址。。但是对每个设备内存布局是不同的。。。作者说单”7200er platform”就有15878个不同版本的系统镜像。。
- Returning to ROMMON
    - Cisco routers use a piece of code called ROMMON as the initially available code to execute after the CPU has been reset.
    - ROMMON is placed the uppermost memory regions. Therefore, its location is known and invariant.
    - 版本少：Taking the 2600 access router platform as an example, there are 8 different versions of ROMMON known to the author.
    - 除了硬件相关的代码之外，没有什么改动，并且已经购买的设备很少受到这个部分代码的改动。。
- ROMMON Uncertainty
    - 当然写exp你还是要对不同的ROMMON做适配，
    - 然而你不一定拿得到目标设备的ROMMON，比如说，设备的第一个版本的系统是固化在里面的，没有升级包存在过。。

- Code Similarity Analysis
- 作者这个工作没有做完。。

Shellcode

- 其实拿到任意代码执行权限之后。。你就可以通过修改内存中的一些信息拿到shell了。
- Arbitrary Services using TCL（sh）:一些设备开始支持一些管理脚本。。
- Ultimate Sniffer:
    - 理论上你当然可以修改系统，让所有的数据包不走fast-path而是由CPU处理，从而sniffer。。。
    - 但是你知道。。其实设备中还有Lawful interception这个功能。。https://en.wikipedia.org/wiki/Lawful_interception%EF%BC%8C%E8%80%8C%E4%B8%94%E8%BF%99%E4%B8%AA%E5%8A%9F%E8%83%BD%E4%B8%8D%E4%BC%9A%E8%A2%AB%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E5%91%98%E8%A7%89%E5%AF%9F%E5%88%B0%E3%80%82%E3%80%82%E3%80%82
- 当然也可以变成MITM，不过可能更麻烦，断TCP连接，并把SEQnumber发送给attacker，让attacker自己来搞定剩下的事。。
- 还有一些功能是路由自己可以做的。。。Selective Redirection，应该是类似DNAT吧。。。