Path Traversal in a Satellite Modem

Simon Greenblatt, *Brown University*

Under the mentorship of Ryan Styles & Tristen Mullins

INTRODUCTION

In April 2021, Tenable disclosed **CVE-2021-20090**, a path traversal vulnerability in the firmware of a Wi-Fi module produced by Arcadyan. This vulnerability allows attackers to bypass authentication to the web interfaces of some home routers. This project focuses on discovering, confirming, understanding, and exploiting this CVE in the **HughesNet HT2000W** Satellite Modem.

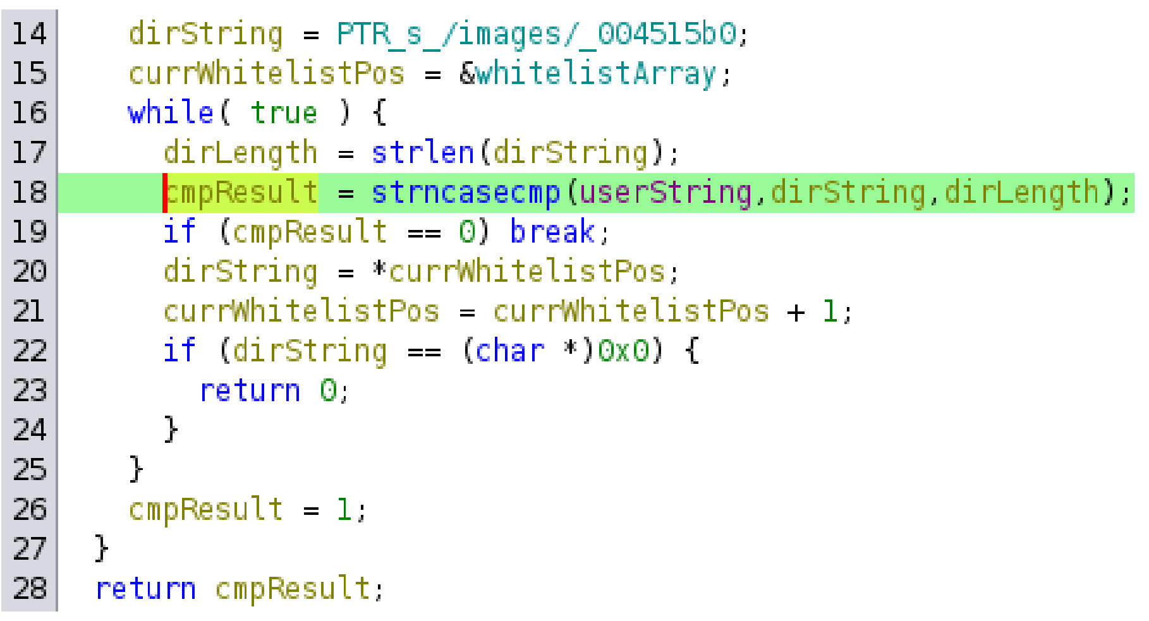
METHODS

1. **Discovery:** We created a hardware and software bill of materials and identified this CVE on the HTTP daemon. We then used a **JTAGulator** to extract the firmware through a UART debug port that wasn't disabled.

2. **Confirmation:** Using **Burp Suite**, we confirmed that the vulnerability was present in the router by modifying GET requests to files in the server that should not have been accessible to an unauthenticated user.

3. **Understanding:** Considering this, used **Ghidra** to reverse engineer the HTTP daemon and identify the faulty check in user-supplied paths (Figure 1).

4. **Exploitation:** Our final exploitation prototype makes use of this CVE alongside other vulnerabilities to gain root access to the device without needing a password.



```
    dirString = PTR_s_/images/_004515b0;
    currWhitelistPos = &whitelistArray;
    while( true ) {
      dirLength = strlen(dirString);
      cmpResult = strncasecmp(userString,dirString,dirLength);
      if (cmpResult == 0) break;
      dirString = *currWhitelistPos;
      currWhitelistPos = currWhitelistPos + 1;
      if (dirString == (char *)0x0) {
        return 0;
      }
    }
    cmpResult = 1;
  }
  return cmpResult;
```

Figure 1: The reverse engineered firmware

RESULTS

Path Traversal: The HTTP daemon contains a whitelist of allowed directories/files that an unauthenticated user can access. However, when checking a user-supplied path, the program will allow any string whose first section matches a string on the whitelist and will ignore anything thereafter. This allows an attacker to perform path traversal by backtracking from an allowed directory using the dot-dot-slash method.

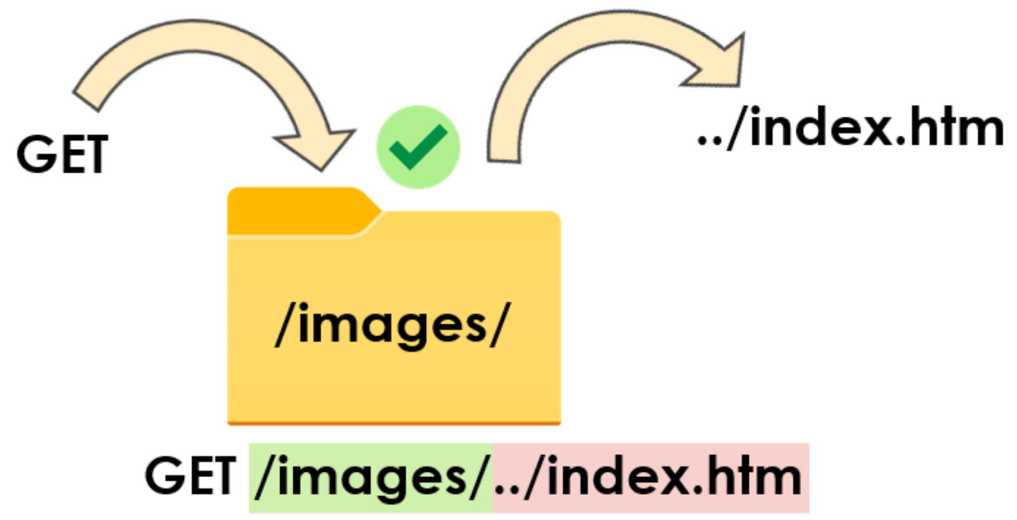
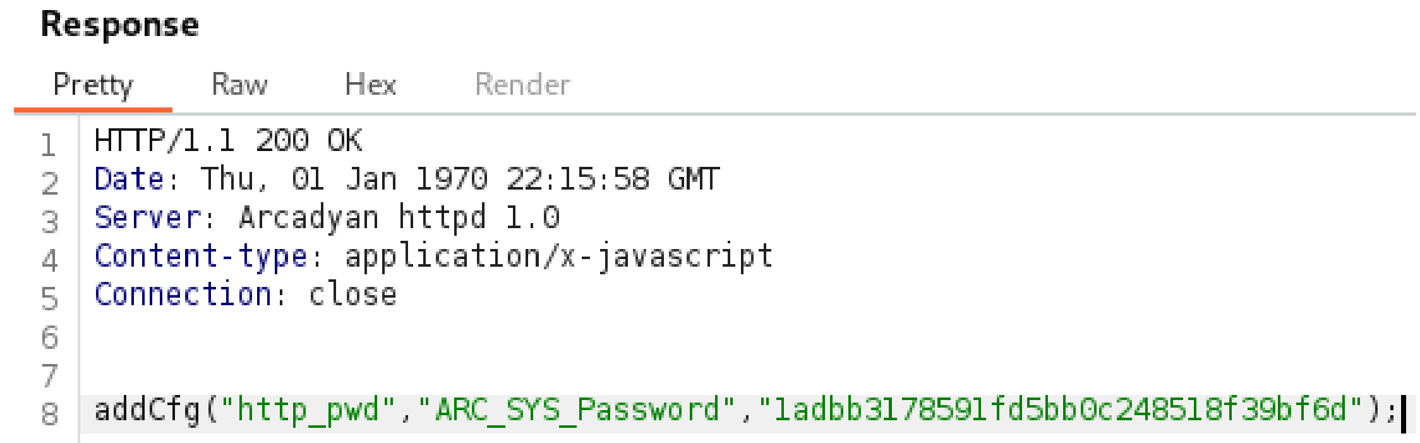


Figure 2: Accessing a file not on the whitelist



Response

Pretty Raw Hex Render

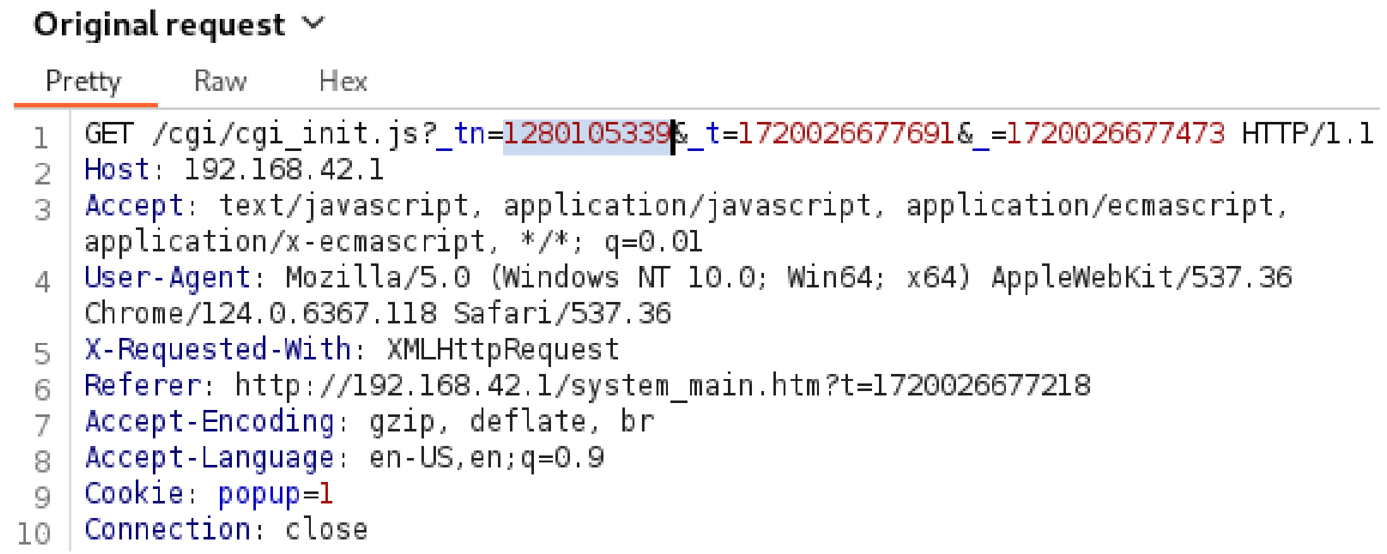
```
HTTP/1.1 200 OK
Date: Thu, 01 Jan 1970 22:15:58 GMT
Server: Arcadyan httpd 1.0
Content-type: application/x-javascript
Connection: close


addCfg("http_pwd","ARC_SYS_Password","1adbb3178591fd5bb0c248518f39bf6d");
```

Figure 3: The router sends the hash of the admin password

Leaking the Hash: The password reset page for the router checks that the user has the current password. This check is done only on the client's side and requires the client to have the hash of the current password. This MD5 hash can be accessed by making a GET request to the *cgi_sys_p.js* JavaScript file.

httoken: Rudimentary authentication within the portal is accomplished using httokens [1]. These are hidden in the document object model for the web pages and must match the httoken in the referer field when making a GET request. Each new page the user accesses contains the httoken needed to request another page.

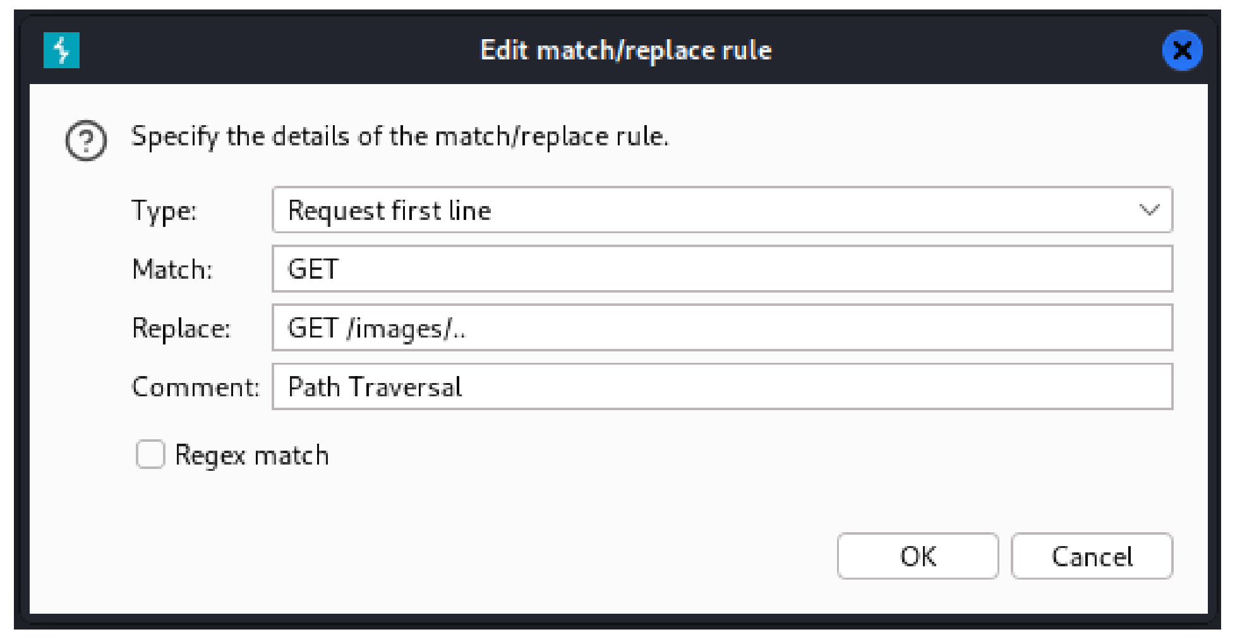


Original request

Pretty Raw Hex

```
GET /cgi/cgi_init.js?_tn=1280105339&_t=1720026677691&_=1720026677473 HTTP/1.1
Host: 192.168.42.1
Accept: text/javascript, application/javascript, application/ecmascript,
application/x-ecmascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Chrome/124.0.6367.118 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://192.168.42.1/system_main.htm?t=1720026677218
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: popup=1
Connection: close
```

Figure 4: Authentication is handled with httokens



Edit match/replace rule

Specify the details of the match/replace rule.

Type: Request first line

Match: GET

Replace: GET /images/..

Comment: Path Traversal

□ Regex match

Figure 5: Proxy rules in Burp Suite can be used to automate the path traversal attack

Putting It All Together: Burp Suite match/replace rules in the proxy can be used to automate the path traversal attack by prepending a string that will pass the whitelist check on every request. We also wrote a Python script that automatically changes the admin password without needing the current password. Gaining access to this portal could allow an attacker to modify firewall settings or redirect network traffic.

DISCUSSION

CVE-2021-20090 is present on millions of devices from at least 13 internet service providers [2]. When disclosing this vulnerability, Tenable had trouble identifying all the vendors that were affected as the number of links in the supply chain that originate from Arcadyan is not known. This vulnerability highlights difficulties in reporting flaws affecting shared libraries, the lack of processes for handling reported vulnerabilities, and the downstream effects it can have on end-users. Incorporating vulnerability management tools into software bills of materials can help keep track of the relationships between vendors and suppliers as well as facilitate the distribution of software patches.

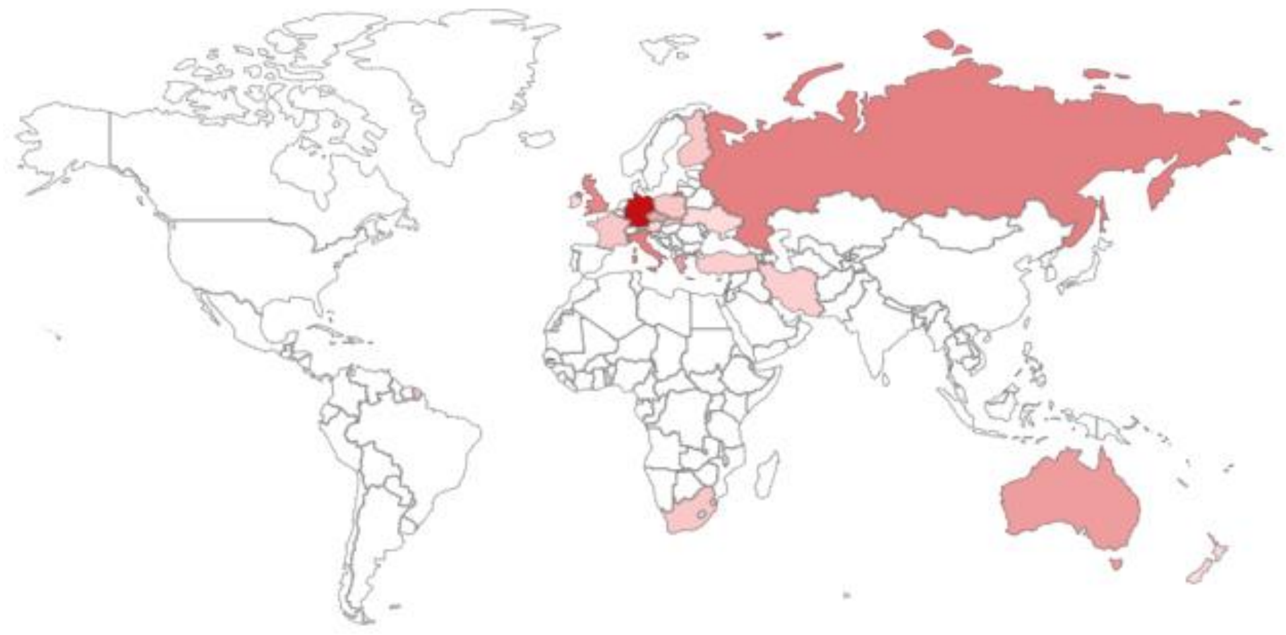


Figure 6: As of July 2024, Shodan lists 807 potential, publicly available devices that could be vulnerable to CVE-2021-20090

REFERENCES

[1] E. Grant, "Bypassing Authentication on Arcadyan Routers with CVE-2021–20090 and rooting some Buffalo", *Medium*, Available: https://medium.com/tenable-techblog/bypassing-authentication-on-arcadyan-routers-with-cve-2021-20090-and-rooting-some-buffalo-ea1dd30980c2

[2] Tenable Research, "Router Vulnerability Present for a Decade: Why IoT Supply Chain is to Blame", Available: https://static.tenable.com/marketing/whitepapers/Whitepaper-Router_Vulnerability_Present _for_a_Decade.pdf

ACKNOWLEDGEMENTS

This research was supported in part by the U.S. Department of Energy Omni Technology Alliance Program, administered by the Oak Ridge Institute for Science and Education.

NATIONAL SECURITY SCIENCES