Talos Vulnerability Report

TALOS-2022-1509

FreshTomato httpd unescape memory corruption vulnerability

JULY 27, 2022

CVE NUMBER

CVE-2022-28665,CVE-2022-28664

Summary

A memory corruption vulnerability exists in the httpd unescape functionality of FreshTomato 2022.1. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.

Tested Versions

FreshTomato 2022.1

Product URLs

FreshTomato - https://www.freshtomato.org/

CVSSv3 Score

5.3 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CWE

CWE-20 - Improper Input Validation

Details

FreshTomato is an open source firmware based on linux. The firmware offers several features for Broadcom-based routers.

The FreshTomato's httpd component has a file named `cgi.c` that contains CGI helper functions. One of these functions is `unescape`:

```
static void unescape(char *s)
{
    unsigned int c;

    while ((s = strpbrk(s, "%+"))) {
[1]
        if (*s == '%') {
            sscanf(s + 1, "%02x", &c);
[2]
            *s++ = (char) c;
[3]
            strcpy(s, s + 2);
[4]
        }
        else if (*s == '+') {
            *s++ = ' ';
        }
    }
}
```

This function takes as argument a string. If URL-encoded, this function will decode it. At `[1]`, there is a loop that takes the next `%` or `+` in the string. If a `%` is found, then at `[2]` the following two characters are converted from hex values to a single character. At `[3]` the converted character replaces the `%` character and the string pointer advance. At `[4]` the string, after the already-parsed URL-encoded character is moved left by two positions, will replace the parsed characters. A string like "A…B%41%42" would go through the following steps:

```
|A|...|B|%|4|1|%|4|2|NULL|          at    [1]/[2]
|A|...|B|A|4|1|%|4|2|NULL|          after [3]
|A|...|B|A|%|4|2|NULL|2|NULL|       after [4]
```

Eventually, after a second iteration of the loop, we would end up like this:

```
|A|...|B|A|B|NULL|2|NULL|2|NULL|    after [4]
```

CVE-2022-28664 - mips branch - httpd unescape memory corruption

The `freshtomato-mips` has a vulnerable URL-decoding feature that can lead to memory corruption. The `unescape` function assumes, wrongly, that after a `%` there are always at least two characters. If this is not the case, the instruction at `[4]` would cause an out-of-bounds read and write.

CVE-2022-28665 - arm branch - httpd unescape memory corruption

The `freshtomato-arm` has a vulnerable URL decoding feature that can lead to memory corruption. The `unescape` function assume, wrongly, that after a `%` there are always at least two characters. If this is not the case, the instruction at `[4]` would cause an out-of-bounds read and write.

Timeline

2022-04-11 - Initial vendor contact
2022-04-27 - Vendor Disclosure
2022-05-06 - Vendor Patch Release
2022-07-27 - Public Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
