Talos Vulnerability Report

TALOS-2022-1553

Abode Systems, Inc. iota All-In-One Security Kit XFINDER information disclosure vulnerability

OCTOBER 20, 2022

CVE NUMBER

CVE-2022-29475

SUMMARY

An information disclosure vulnerability exists in the XFINDER functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

abode systems, inc. iota All-In-One Security Kit 6.9X
abode systems, inc. iota All-In-One Security Kit 6.9Z

PRODUCT URLS

iota All-In-One Security Kit - https://goabode.com/product/iota-security-kit

CVSSV3 SCORE

4.7 - CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N

CWE

CWE-294 - Authentication Bypass by Capture-replay

DETAILS

The iota All-In-One Security Kit is a home security gateway containing an HD camera, infrared motion detection sensor, Ethernet, WiFi and Cellular connectivity. The iota gateway orchestrates communications between sensors (cameras, door and window alarms, motion detectors, etc.) distributed on the LAN and the abode cloud. Users of the iota can communicate with the device through mobile application or web application.

The `iota` device exposes a service on UDP/55030 which is referenced throughout the `/root/hpgw` binary as the 'XFINDER' service. The apparent intent of this service is to allow XFINDER devices to discover and interact with each other over the local network. The XFINDER protocol is not in cleartext, opting to slightly obfuscate the data via XOR with a static key.

The function responsible for the XOR enciphering is located at offset `0x179460` of the `/root/hpgw` binary from version 6.9Z. We have chosen to refer to this function as `xfinder_xor`

The decompilation of this function is included for reference:

```
int __fastcall xfinder_xor(char *buff, int buff_size)
{
  int idx; // r3

  for ( idx = 0; idx < buff_size; ++idx )
    buff[idx] = xfinder_secret_key[idx & 0x3F] ^ ~buff[idx];
  return 0;
}
```

To discover XFINDER `panel` devices on your network, one can encipher and broadcast `SEARCH /panel FINDER/1.0\r\n` on UDP/55030. Similarly, to discover `ipcam` devices, `SEARCH /ipcam FINDER/1.0\r\n` can be broadcast.

Any XFINDER devices on the network that are configured to respond to `/panel` or `/ipcam` will reply directly, providing various details like their name, hardware and software versions, network configuration, and the status of their web interface.

Similarly, some parameters of XFINDER devices can be configured by enciphering and transmitting a `CONFIG /panel FINDER/1.0` command.

For example, to enable the embedded web server on an `iota` device, submit the following to the target device on UDP/55030:

```
CONFIG /panel FINDER/1.0
MAC: B0:C5:CA:00:00:00
Auth: {MD5(username:password)}
WebEnable: 1
```

An attacker who can monitor XFINDER traffic while configuration changes are in-progress, and who has knowledge of the static XOR key, can extract the `Auth` field and replay that value to make other configuration changes to the device.

One might be inclined to attempt to crack the MD5 hash. The default username is `abodeservice15` and the password on the test device is 16 characters long, made up of digits and uppercase and lowercase letters. Cracking attempts are unlikely to be successful.

TIMELINE

2022-07-13 - Initial Vendor Contact
2022-07-14 - Vendor Disclosure
2022-10-20 - Public Release

CREDIT

Discovered by Matt Wiseman of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2022-1561

NEXT REPORT

TALOS-2022-1562