# CVE Detail – CVE-2019-13398

Dynacolor FCM-MB40 v1.2.0.0 devices allow remote attackers to execute arbitrary commands via a crafted parameter to a CGI script, as demonstrated by sed injection in cgi-bin/camctrl\_save\_profile.cgi (save parameter) and cgi-bin/ddns.cgi.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.86769

## CVSS Scoring

CVSS v3.0 Score: 7.2

Severity: HIGH

## Mapped CWE(s)

* CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

## CAPEC(s)

* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-15: Command Delimiters
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-6: Argument Injection
* CAPEC-88: OS Command Injection

## Affected Products

* cpe:2.3:o:fortinet:fcm-mb40\_firmware:1.2.0.0:\*:\*:\*:\*:\*:\*:\*