PSIRT

Stack-based buffer overflow vulnerability in API

IR Number	FG-IR-25-254
Published Date	May 13, 2025
Component	OTHERS
Severity	Critical
CVSSv3 Score	9.6
Impact	Execute unauthorized code or commands
CVE ID	CVE-2025-32756
Download	CVRF CSAF STIX

- Scan the device network
- Erase system crashlogs
- Enable fcgi debugging to log credentials from the system or SSH login attempts

See IoCs below for more information

Version	Affected	Solution
FortiCamera 2.1	2.1.0 through 2.1.3	Upgrade to 2.1.4 or above
FortiCamera 2.0	2.0 all versions	Migrate to a fixed release
FortiCamera 1.1	1.1 all versions	Migrate to a fixed release
FortiMail 7.6	7.6.0 through 7.6.2	Upgrade to 7.6.3 or above
FortiMail 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiMail 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiMail 7.0	7.0.0 through 7.0.8	Upgrade to 7.0.9 or above
FortiNDR 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiNDR 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
FortiNDR 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.5 or above
FortiNDR 7.0	7.0.0 through 7.0.6	Upgrade to 7.0.7 or above
FortiRecorder 7.2	7.2.0 through 7.2.3	Upgrade to 7.2.4 or above
FortiRecorder 7.0	7.0.0 through 7.0.5	Upgrade to 7.0.6 or above

Logs

The following log entries are possible IOCs:

Output of CLI command 'diagnose debug application httpd display trace-log':
[x x x x:x:x.x 2025] [fcgid:warn] [pid 1829] [client x.x.x.x:x] mod_fcgid: error reading data, FastCGI server closed connection
[x x x x:x:x.x 2025] [fcgid:error] [pid 1503] mod_fcgid: process /migadmin/www/fcgi/admin.fe(1741) exit(communication error), get unexpected signal 11

IP Addresses

The Threat Actor (TA) has been seen using the following IP addresses:
198.105.127.124
43.228.217.173
43.228.217.82
156.236.76.90
218.187.69.244
218.187.69.59

Modified Settings

To verify if fcgi debugging is enabled on your system, use the following CLI command:

```
diag debug application fcgi
```

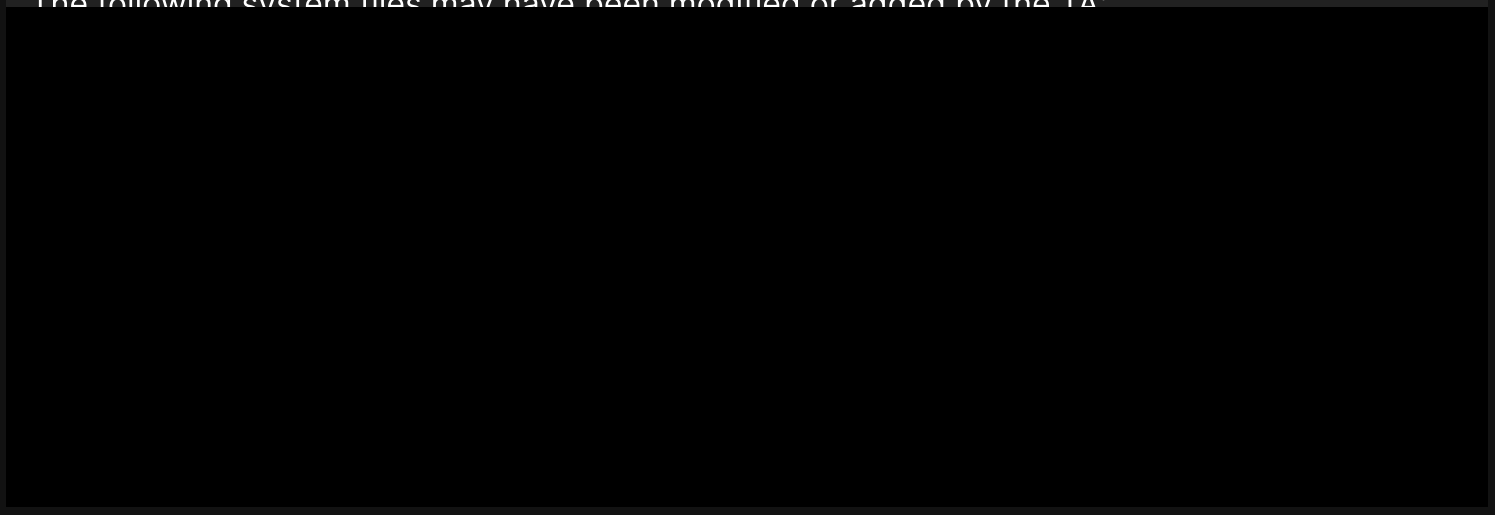
If the output shows "general to-file ENABLED", it means fcgi debugging is enabled on your system:

```
fcgi debug level is 0x80041
general to-file ENABLED
```

This is not a default setting, so unless you have enabled it in the past, this is potentially an Indicator of Compromise

Files

The following system files may have been modified or added by the TA:



```
/dev/null >/var/spool/crashlog/fcgi.debug
```

- [Added File] /var/spool/.sync - Credentials are gathered into this file by the cron jobs above
- /etc/pam.d/sshd - Lines were added to it to include malicious libfmlogin.so below
- [Added File] /lib/libfmlogin.so - MD5:364929c45703a84347064e2d5de45bcd - malicious library that logs username and password using SSH login
- [Added File] /tmp/.sshdpm - contains credentials gathered by /lib/libfmlogin.so above
- [Added File] /bin/fmtest - MD5: 2c8834a52faee8d87cff7cd09c4fb946 - Script to scan the network
- /etc/httpd.conf - A line was added to include socks.so: LoadModule socks5_module modules/mod_socks5.so

Workaround

Disable HTTP/HTTPS administrative and portal interface

Acknowledgement

Discovered by Théo Leleu and David Maciejak of Fortinet Product Security Team based on threat activity.

Timeline

2025-05-13: Initial publication
2025-05-13: Format