CVE-2025-32756 – Fortinet Zero-Day Exploitation: Indicators of Compromise (IOCs)

The following indicators have been observed in active exploitation of CVE-2025-32756. This reference sheet can be used by incident response and SOC teams to detect signs of compromise across affected Fortinet systems.

Log-Based Indicators

Run this CLI command on Fortinet devices:

```
diagnose debug application httpd display trace-log
```

Look for log entries such as:

```
[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
```

Threat Actor IP Addresses

Monitor for communications with 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 Debug Settings

Run this command to check for unexpected fcgi debug settings:

```
diag debug application fcgi
```

Output indicating compromise:

fcgi debug level is 0x80041
general to-file ENABLED

Malicious Files and Persistence Artifacts

File Path	Description	MD5 (if known)
/bin/wpad_ac_helper	Main malware file	4410352e110f82eabc0bf160bec41d21
/bin/busybox	Malicious utility binary	ebce43017d2cb316ea45e08374de7315, 489821c38f429a21e1ea821f8460e590
/data/etc/crontab	Credential harvesting cron job	
/var/spool/cron/crontabs/root	Credential backup cron job	
/var/spool/.sync	Credential output file	
/lib/libfmlogin.so	SSH login capture PAM module	364929c45703a84347064e2d5de45bcd
/tmp/.sshdpm	Credential capture cache	
/bin/fmtest	Internal network scanner	2c8834a52faee8d87cff7cd09c4fb946
/etc/pam.d/sshd	Modified PAM configuration	
/etc/httpd.conf	Modified to load malicious module	

Use this sheet to audit Fortinet appliances and infrastructure components for signs of intrusion.