PSIRT

Heap-based buffer overflow in cw_acd daemon

IR Number	FG-IR-25-084
Published Date	Jan 13, 2026
Updated Date	Jan 19, 2026
Component	OTHERS
Severity	High
CVSSv3 Score	7.4
Impact	Execute unauthorized code or commands
CVE ID	CVE-2025-25249
Download	CVRF CSAF

Version	Affected	Solution
FortiOS 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiOS 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
FortiOS 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiOS 7.0	7.0.0 through 7.0.17	Upgrade to 7.0.18 or above
FortiOS 6.4	6.4.0 through 6.4.16	Upgrade to upcoming 6.4.17 or above
FortiSwitchManager 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiSwitchManager 7.0	7.0.0 through 7.0.5	Upgrade to 7.0.6 or above

Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

Workarrounds :

For each interface, remove "fabric" access. For example change :
config system interface
edit "port1"
set allowaccess fabric ssh https
next
end

to :
config system interface
edit "port1"
set allowaccess ssh https
next
end

```
set member "my_allowed_addresses"
end
config firewall local-in-policy
edit 1 (allow from trusted devices)
set intf "port1" (where fabric is enabled)
set srcaddr "CAPWAP_DEVICES_IPs"
set dstaddr "all"
set service "CAPWAP-CONTROL"
set schedule "always"
set action accept
next
edit 2 (block everyone else)
set intf "port1" (where fabric is enabled)
set srcaddr "all'
set dstaddr "all"
set service "CAPWAP-CONTROL"
set schedule "always"
set action deny
next
end
```

Acknowledgement

Internally discovered and reported by Gwendal Guégniaud of Fortinet Product Security Team.

Timeline

2026-01-13: Initial publication