VMware Vulnerabilities - IOC Reference Worksheet

Overview

This document provides detailed indicators of compromise (IOCs) for VMware vulnerabilities disclosed in May 2025 (CVE-2025-41225 through CVE-2025-41231). These IOCs can assist security teams in identifying potential exploitation attempts within vCenter Server, ESXi, VMware Workstation, Fusion, and Cloud Foundation.

IOC: URL Path Analysis

IOC Path	Product(s)	Purpose / Risk	Log Location	Threat Use Case
/ui/#/login	vCenter Server	Login interface for vCenter; potential target for reflected XSS (CVE-2025-41228).	vSphere UI log, reverse proxy logs	Session hijacking, redirection, or reflected XSS.
/mob	vCenter Server	Managed Object Browser for internal API enumeration.	vsphere-client logs, reverse proxy logs	Reconnaissance, unauthorized object access.
/login	vCenter Server, ESXi	Generic login endpoint; may support token or legacy session auth.	Web access logs, WAF/IDS logs	Credential stuffing, brute-force, session abuse.
/cfg	ESXi Web UI	Potential configuration/debug endpoint. Possible target for directory traversal (CVE-2025-41229).	ESXi access logs, proxy/WAF logs	Directory traversal, unauthorized config file access.

Additional Indicators of Compromise

IOC Type	Details
Script	`alarm.sh` with custom parameters or abnormal execution patterns from scripts in vCenter.
Port	`443/tcp` – commonly targeted for exposed ESXi, vCenter, or Cloud Foundation services.
Behavior	Unexpected guest operation failures, high memory consumption from guest OS, script-based alarms triggering actions.

Log Artifact	Log entries like `unauthorized access`, `script execution failed`, or `guest operation aborted` in vCenter and ESXi logs.

SIEM Use Cases

Monitor access logs, WAF events, and syslog data ingested by your SIEM for signs of abnormal access to these paths. Queries should filter for unauthorized or anomalous requests to these endpoints, especially if accompanied by suspicious parameters such as '?redirect=' or embedded JavaScript payloads. Also monitor for abnormal script execution, memory usage, and authentication anomalies.