

Findings Report

Acme Corp (Demo) · Generated Tue, 29 Sep 2026 13:37:40 GMT

Severity summary

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
48	36	30	12	12	138

Triage tiers

monitor: 36 | info: 12 | act_now: 60 | plan: 30

Findings

SEVERITY	TITLE	HOST	CVE	CVSS	TIER	STATUS	LAST SEEN
CRITICAL	Apache Struts OGNL Injection (CVE-2017-5638) KEV	203.0.113.41:80	CVE-2017-5638	10	act_now	fixed	2026-09-27
CRITICAL	Apache Struts OGNL Injection (CVE-2017-5638) KEV	198.51.100.28:80	CVE-2017-5638	10	act_now	fixed	2026-09-27
CRITICAL	Apache Struts OGNL Injection (CVE-2017-5638) KEV	203.0.113.19:80	CVE-2017-5638	10	act_now	fixed	2026-09-17
CRITICAL	Apache Struts OGNL Injection (CVE-2017-5638) KEV	198.51.100.17:80	CVE-2017-5638	10	act_now	fixed	2026-09-17
CRITICAL	Apache Struts OGNL Injection (CVE-2017-5638) KEV	192.0.2.10:80	CVE-2017-5638	10	act_now	fixed	2026-09-07
CRITICAL	Apache Struts OGNL Injection (CVE-2017-5638) KEV	203.0.113.6:80	CVE-2017-5638	10	act_now	fixed	2026-09-07
CRITICAL	Apache Log4j Remote Code Execution (CVE-2021-44228) KEV	192.0.2.34:8080	CVE-2021-44228	10	act_now	fix_pending_verification	2026-09-29
CRITICAL	Apache Log4j Remote Code Execution (CVE-2021-44228) KEV	192.0.2.11:8080	CVE-2021-44228	10	act_now	fix_pending_verification	2026-09-29
CRITICAL	Apache Log4j Remote Code Execution (CVE-2021-44228) KEV	198.51.100.9:8080	CVE-2021-44228	10	act_now	fix_pending_verification	2026-09-19
CRITICAL	Apache Log4j Remote Code Execution (CVE-2021-44228) KEV	192.0.2.22:8080	CVE-2021-44228	10	act_now	fix_pending_verification	2026-09-19
CRITICAL	Apache Log4j Remote Code Execution (CVE-2021-44228) KEV	198.51.100.4:8080	CVE-2021-44228	10	act_now	fix_pending_verification	2026-09-09
CRITICAL	Apache Log4j Remote Code Execution (CVE-2021-44228) KEV	192.0.2.15:8080	CVE-2021-44228	10	act_now	fix_pending_verification	2026-09-09
CRITICAL	OpenSSL Heartbleed (CVE-2014-0160) KEV	192.0.2.22:443	CVE-2014-0160	9.8	act_now	vulnerable	2026-09-29
CRITICAL	OpenSSL Heartbleed (CVE-2014-0160) KEV	192.0.2.10:443	CVE-2014-0160	9.8	act_now	vulnerable	2026-09-29
CRITICAL	OpenSSL Heartbleed (CVE-2014-0160) KEV	198.51.100.4:443	CVE-2014-0160	9.8	act_now	vulnerable	2026-09-21
CRITICAL	OpenSSL Heartbleed (CVE-2014-0160) KEV	192.0.2.15:443	CVE-2014-0160	9.8	act_now	vulnerable	2026-09-21
CRITICAL	OpenSSL Heartbleed (CVE-2014-0160) KEV	192.0.2.34:443	CVE-2014-0160	9.8	act_now	vulnerable	2026-09-11
CRITICAL	OpenSSL Heartbleed (CVE-2014-0160) KEV	192.0.2.11:443	CVE-2014-0160	9.8	act_now	vulnerable	2026-09-11
CRITICAL	Atlassian Confluence RCE (CVE-2022-26134) KEV	198.51.100.9:8090	CVE-2022-26134	9.8	act_now	vulnerable	2026-09-25
CRITICAL	Atlassian Confluence RCE (CVE-2022-26134) KEV	192.0.2.22:8090	CVE-2022-26134	9.8	act_now	vulnerable	2026-09-25
CRITICAL	Atlassian Confluence RCE (CVE-2022-26134) KEV	198.51.100.28:8090	CVE-2022-26134	9.8	act_now	vulnerable	2026-09-15
CRITICAL	Atlassian Confluence RCE (CVE-2022-26134) KEV	198.51.100.4:8090	CVE-2022-26134	9.8	act_now	vulnerable	2026-09-15
CRITICAL	Atlassian Confluence RCE (CVE-2022-26134) KEV	198.51.100.17:8090	CVE-2022-26134	9.8	act_now	vulnerable	2026-09-05

SEVERITY	TITLE	HOST	CVE	CVSS	TIER	STATUS	LAST SEEN
CRITICAL	Atlassian Confluence RCE (CVE-2022-26134) KEV	192.0.2.34:8090	CVE-2022-26134	9.8	act_now	vulnerable	2026-09-05
CRITICAL	vsftpd Backdoor (CVE-2011-2523) KEV	198.51.100.4:21	CVE-2011-2523	9.8	act_now	vulnerable	2026-09-27
CRITICAL	vsftpd Backdoor (CVE-2011-2523) KEV	192.0.2.15:21	CVE-2011-2523	9.8	act_now	vulnerable	2026-09-27
CRITICAL	vsftpd Backdoor (CVE-2011-2523) KEV	198.51.100.17:21	CVE-2011-2523	9.8	act_now	vulnerable	2026-09-17
CRITICAL	vsftpd Backdoor (CVE-2011-2523) KEV	192.0.2.34:21	CVE-2011-2523	9.8	act_now	vulnerable	2026-09-17
CRITICAL	vsftpd Backdoor (CVE-2011-2523) KEV	198.51.100.9:21	CVE-2011-2523	9.8	act_now	vulnerable	2026-09-07
CRITICAL	vsftpd Backdoor (CVE-2011-2523) KEV	192.0.2.22:21	CVE-2011-2523	9.8	act_now	vulnerable	2026-09-07
CRITICAL	VMware vCenter RCE (CVE-2021-21972) KEV	203.0.113.6:443	CVE-2021-21972	9.8	act_now	vulnerable	2026-09-29
CRITICAL	VMware vCenter RCE (CVE-2021-21972) KEV	198.51.100.9:443	CVE-2021-21972	9.8	act_now	vulnerable	2026-09-29
CRITICAL	VMware vCenter RCE (CVE-2021-21972) KEV	198.51.100.28:443	CVE-2021-21972	9.8	act_now	vulnerable	2026-09-21
CRITICAL	VMware vCenter RCE (CVE-2021-21972) KEV	198.51.100.4:443	CVE-2021-21972	9.8	act_now	vulnerable	2026-09-21
CRITICAL	VMware vCenter RCE (CVE-2021-21972) KEV	203.0.113.19:443	CVE-2021-21972	9.8	act_now	vulnerable	2026-09-11
CRITICAL	VMware vCenter RCE (CVE-2021-21972) KEV	198.51.100.17:443	CVE-2021-21972	9.8	act_now	vulnerable	2026-09-11
HIGH	Outdated Apache httpd 2.4.49 Path Traversal (CVE-2021-41773) KEV	192.0.2.22:80	CVE-2021-41773	7.5	act_now	fixed	2026-09-25
HIGH	Outdated Apache httpd 2.4.49 Path Traversal (CVE-2021-41773) KEV	198.51.100.9:80	CVE-2021-41773	7.5	act_now	fixed	2026-09-25
HIGH	Outdated Apache httpd 2.4.49 Path Traversal (CVE-2021-41773) KEV	198.51.100.4:80	CVE-2021-41773	7.5	act_now	fixed	2026-09-15
HIGH	Outdated Apache httpd 2.4.49 Path Traversal (CVE-2021-41773) KEV	192.0.2.15:80	CVE-2021-41773	7.5	act_now	fixed	2026-09-15
HIGH	Outdated Apache httpd 2.4.49 Path Traversal (CVE-2021-41773) KEV	192.0.2.34:80	CVE-2021-41773	7.5	act_now	fixed	2026-09-05
HIGH	Outdated Apache httpd 2.4.49 Path Traversal (CVE-2021-41773) KEV	192.0.2.11:80	CVE-2021-41773	7.5	act_now	fixed	2026-09-05
CRITICAL	Spring4Shell (CVE-2022-22965)	203.0.113.19:8080	CVE-2022-22965	9.8	act_now	fixed	2026-09-29
CRITICAL	Spring4Shell (CVE-2022-22965)	198.51.100.17:8080	CVE-2022-22965	9.8	act_now	fixed	2026-09-29
CRITICAL	Spring4Shell (CVE-2022-22965)	203.0.113.6:8080	CVE-2022-22965	9.8	act_now	fixed	2026-09-19
CRITICAL	Spring4Shell (CVE-2022-22965)	198.51.100.9:8080	CVE-2022-22965	9.8	act_now	fixed	2026-09-19
CRITICAL	Spring4Shell (CVE-2022-22965)	203.0.113.41:8080	CVE-2022-22965	9.8	act_now	fixed	2026-09-09
CRITICAL	Spring4Shell (CVE-2022-22965)	198.51.100.28:8080	CVE-2022-22965	9.8	act_now	fixed	2026-09-09
CRITICAL	Unauthenticated Redis Access	198.51.100.17:6379	—	9.1	act_now	vulnerable	2026-09-23
CRITICAL	Unauthenticated Redis Access	192.0.2.34:6379	—	9.1	act_now	vulnerable	2026-09-23
CRITICAL	Unauthenticated Redis Access	203.0.113.6:6379	—	9.1	act_now	vulnerable	2026-09-13
CRITICAL	Unauthenticated Redis Access	198.51.100.9:6379	—	9.1	act_now	vulnerable	2026-09-13
CRITICAL	Unauthenticated Redis Access	198.51.100.28:6379	—	9.1	act_now	vulnerable	2026-09-03
CRITICAL	Unauthenticated Redis Access	198.51.100.4:6379	—	9.1	act_now	vulnerable	2026-09-03
HIGH	Exposed Docker Remote API	192.0.2.10:2375	—	8.6	plan	vulnerable	2026-09-25
HIGH	Exposed Docker Remote API	203.0.113.6:2375	—	8.6	plan	vulnerable	2026-09-25

SEVERITY	TITLE	HOST	CVE	CVSS	TIER	STATUS	LAST SEEN
HIGH	Exposed Docker Remote API	203.0.113.41:2375	—	8.6	plan	vulnerable	2026-09-15
HIGH	Exposed Docker Remote API	198.51.100.28:2375	—	8.6	plan	vulnerable	2026-09-15
HIGH	Exposed Docker Remote API	192.0.2.11:2375	—	8.6	plan	vulnerable	2026-09-05
HIGH	Exposed Docker Remote API	203.0.113.19:2375	—	8.6	plan	vulnerable	2026-09-05
HIGH	MongoDB Unauthenticated Access	192.0.2.34:27017	—	8.1	act_now	vulnerable	2026-09-23
HIGH	MongoDB Unauthenticated Access	198.51.100.17:27017	—	8.1	act_now	vulnerable	2026-09-23
HIGH	MongoDB Unauthenticated Access	198.51.100.9:27017	—	8.1	act_now	vulnerable	2026-09-13
HIGH	MongoDB Unauthenticated Access	192.0.2.22:27017	—	8.1	act_now	vulnerable	2026-09-13
HIGH	MongoDB Unauthenticated Access	198.51.100.4:27017	—	8.1	act_now	vulnerable	2026-09-03
HIGH	MongoDB Unauthenticated Access	192.0.2.15:27017	—	8.1	act_now	vulnerable	2026-09-03
HIGH	SMB Signing Not Required	192.0.2.15:445	—	7.8	plan	vulnerable	2026-09-27
HIGH	SMB Signing Not Required	198.51.100.4:445	—	7.8	plan	vulnerable	2026-09-27
HIGH	SMB Signing Not Required	192.0.2.34:445	—	7.8	plan	vulnerable	2026-09-17
HIGH	SMB Signing Not Required	192.0.2.11:445	—	7.8	plan	vulnerable	2026-09-17
HIGH	SMB Signing Not Required	192.0.2.22:445	—	7.8	plan	vulnerable	2026-09-07
HIGH	SMB Signing Not Required	192.0.2.10:445	—	7.8	plan	vulnerable	2026-09-07
HIGH	TLS 1.0 Enabled (Deprecated)	192.0.2.10:443	—	7.4	plan	vulnerable	2026-09-29
HIGH	TLS 1.0 Enabled (Deprecated)	192.0.2.22:443	—	7.4	plan	vulnerable	2026-09-29
HIGH	TLS 1.0 Enabled (Deprecated)	192.0.2.15:443	—	7.4	plan	vulnerable	2026-09-21
HIGH	TLS 1.0 Enabled (Deprecated)	203.0.113.41:443	—	7.4	plan	vulnerable	2026-09-21
HIGH	TLS 1.0 Enabled (Deprecated)	192.0.2.11:443	—	7.4	plan	vulnerable	2026-09-11
HIGH	TLS 1.0 Enabled (Deprecated)	203.0.113.19:443	—	7.4	plan	vulnerable	2026-09-11
HIGH	SSH Weak Key Exchange Algorithms	192.0.2.11:22	—	7.2	plan	vulnerable	2026-09-29
HIGH	SSH Weak Key Exchange Algorithms	192.0.2.34:22	—	7.2	plan	vulnerable	2026-09-29
HIGH	SSH Weak Key Exchange Algorithms	192.0.2.22:22	—	7.2	plan	vulnerable	2026-09-19
HIGH	SSH Weak Key Exchange Algorithms	192.0.2.10:22	—	7.2	plan	vulnerable	2026-09-19
HIGH	SSH Weak Key Exchange Algorithms	192.0.2.15:22	—	7.2	plan	vulnerable	2026-09-09
HIGH	SSH Weak Key Exchange Algorithms	203.0.113.41:22	—	7.2	plan	vulnerable	2026-09-09
MEDIUM	SNMP Public Community String	203.0.113.19:161	—	6.5	plan	vulnerable	2026-09-23
MEDIUM	SNMP Public Community String	198.51.100.17:161	—	6.5	plan	vulnerable	2026-09-23
MEDIUM	SNMP Public Community String	203.0.113.6:161	—	6.5	plan	vulnerable	2026-09-13
MEDIUM	SNMP Public Community String	192.0.2.10:161	—	6.5	plan	vulnerable	2026-09-13
MEDIUM	SNMP Public Community String	203.0.113.41:161	—	6.5	plan	vulnerable	2026-09-03
MEDIUM	SNMP Public Community String	198.51.100.28:161	—	6.5	plan	vulnerable	2026-09-03
MEDIUM	SMTP Open Relay Suspected	198.51.100.28:25	—	6.5	monitor	vulnerable	2026-09-27
MEDIUM	SMTP Open Relay Suspected	198.51.100.4:25	—	6.5	monitor	vulnerable	2026-09-27
MEDIUM	SMTP Open Relay Suspected	198.51.100.17:25	—	6.5	monitor	vulnerable	2026-09-17
MEDIUM	SMTP Open Relay Suspected	203.0.113.19:25	—	6.5	monitor	vulnerable	2026-09-17
MEDIUM	SMTP Open Relay Suspected	203.0.113.6:25	—	6.5	monitor	vulnerable	2026-09-07
MEDIUM	SMTP Open Relay Suspected	198.51.100.9:25	—	6.5	monitor	vulnerable	2026-09-07
MEDIUM	HTTP Missing Content-Security-Policy	198.51.100.9:443	—	5.3	monitor	vulnerable	2026-09-29
MEDIUM	Directory Listing Enabled	198.51.100.17:80	—	5.3	monitor	vulnerable	2026-09-29
MEDIUM	HTTP Missing Content-Security-Policy	192.0.2.22:443	—	5.3	monitor	vulnerable	2026-09-29
MEDIUM	Directory Listing Enabled	192.0.2.34:80	—	5.3	monitor	vulnerable	2026-09-29
MEDIUM	HTTP Missing Content-Security-Policy	198.51.100.4:443	—	5.3	monitor	vulnerable	2026-09-21
MEDIUM	HTTP Missing Content-Security-Policy	198.51.100.28:443	—	5.3	monitor	vulnerable	2026-09-21
MEDIUM	Directory Listing Enabled	198.51.100.9:80	—	5.3	monitor	vulnerable	2026-09-19
MEDIUM	Directory Listing Enabled	203.0.113.6:80	—	5.3	monitor	vulnerable	2026-09-19
MEDIUM	HTTP Missing Content-Security-Policy	198.51.100.17:443	—	5.3	monitor	vulnerable	2026-09-11

SEVERITY	TITLE	HOST	CVE	CVSS	TIER	STATUS	LAST SEEN
MEDIUM	HTTP Missing Content-Security-Policy	192.0.2.34:443	—	5.3	monitor	vulnerable	2026-09-11
MEDIUM	Directory Listing Enabled	198.51.100.28:80	—	5.3	monitor	vulnerable	2026-09-09
MEDIUM	Directory Listing Enabled	198.51.100.4:80	—	5.3	monitor	vulnerable	2026-09-09
MEDIUM	TLS Certificate Expires < 30 Days	203.0.113.6:443	—	5	monitor	vulnerable	2026-09-25
MEDIUM	TLS Certificate Expires < 30 Days	198.51.100.9:443	—	5	monitor	vulnerable	2026-09-25
MEDIUM	TLS Certificate Expires < 30 Days	198.51.100.28:443	—	5	monitor	vulnerable	2026-09-15
MEDIUM	TLS Certificate Expires < 30 Days	203.0.113.41:443	—	5	monitor	vulnerable	2026-09-15
MEDIUM	TLS Certificate Expires < 30 Days	203.0.113.19:443	—	5	monitor	vulnerable	2026-09-05
MEDIUM	TLS Certificate Expires < 30 Days	198.51.100.17:443	—	5	monitor	vulnerable	2026-09-05
LOW	TLS Certificate Hostname Mismatch	192.0.2.15:443	—	3.7	monitor	still_vulnerable	2026-09-27
LOW	TLS Certificate Hostname Mismatch	203.0.113.41:443	—	3.7	monitor	still_vulnerable	2026-09-27
LOW	TLS Certificate Hostname Mismatch	192.0.2.11:443	—	3.7	monitor	still_vulnerable	2026-09-17
LOW	TLS Certificate Hostname Mismatch	203.0.113.19:443	—	3.7	monitor	still_vulnerable	2026-09-17
LOW	TLS Certificate Hostname Mismatch	192.0.2.10:443	—	3.7	monitor	still_vulnerable	2026-09-07
LOW	TLS Certificate Hostname Mismatch	192.0.2.22:443	—	3.7	monitor	still_vulnerable	2026-09-07
INFO	Open Port: 8080 (HTTP Alt)	192.0.2.22:8080	—	—	info	vulnerable	2026-09-25
INFO	Open Port: 8080 (HTTP Alt)	192.0.2.10:8080	—	—	info	vulnerable	2026-09-25
INFO	NTP Mode 6 Queries	192.0.2.34:123	—	—	info	vulnerable	2026-09-23
INFO	NTP Mode 6 Queries	192.0.2.11:123	—	—	info	vulnerable	2026-09-23
INFO	Open Port: 8080 (HTTP Alt)	192.0.2.15:8080	—	—	info	vulnerable	2026-09-15
INFO	Open Port: 8080 (HTTP Alt)	203.0.113.41:8080	—	—	info	vulnerable	2026-09-15
INFO	NTP Mode 6 Queries	192.0.2.22:123	—	—	info	vulnerable	2026-09-13
INFO	NTP Mode 6 Queries	192.0.2.10:123	—	—	info	vulnerable	2026-09-13
INFO	Open Port: 8080 (HTTP Alt)	192.0.2.11:8080	—	—	info	vulnerable	2026-09-05
INFO	Open Port: 8080 (HTTP Alt)	192.0.2.34:8080	—	—	info	vulnerable	2026-09-05
INFO	NTP Mode 6 Queries	192.0.2.15:123	—	—	info	vulnerable	2026-09-03
INFO	NTP Mode 6 Queries	198.51.100.4:123	—	—	info	vulnerable	2026-09-03
LOW	ICMP Timestamp Disclosure	192.0.2.11	—	2.1	monitor	vulnerable	2026-09-29
LOW	ICMP Timestamp Disclosure	203.0.113.19	—	2.1	monitor	vulnerable	2026-09-29
LOW	ICMP Timestamp Disclosure	192.0.2.10	—	2.1	monitor	vulnerable	2026-09-19
LOW	ICMP Timestamp Disclosure	203.0.113.6	—	2.1	monitor	vulnerable	2026-09-19
LOW	ICMP Timestamp Disclosure	203.0.113.41	—	2.1	monitor	vulnerable	2026-09-09
LOW	ICMP Timestamp Disclosure	192.0.2.15	—	2.1	monitor	vulnerable	2026-09-09