

The TrustKeeper vulnerability and policy scan is designed to assess the network, service, and application security of your on-line systems.

The vulnerability and policy scan also assesses compliance with configuration requirements of applicable Information Security standards. Note that a full vulnerability assessment may require manual penetration testing where more aggressive techniques can be utilized to test the security of your systems.

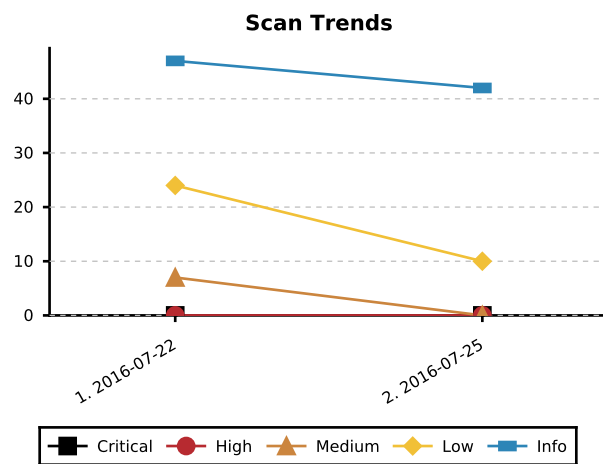
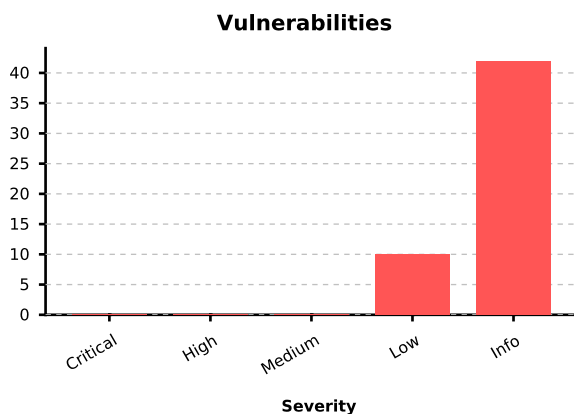
On 2016-07-25, Trustwave's TrustKeeper vulnerability scanner performed a network-based assessment of the target devices of HEMKO Systems Corporation to identify security vulnerabilities. A total of 52 vulnerabilities were found during the scan.

Trustwave uses the following risk ranking when reporting vulnerability risks:

- Critical risk vulnerabilities indicate that a system can be successfully attacked. You should investigate and remediate these issues immediately.
- High risk vulnerabilities indicate problems that could result in immediate compromise. These issues should be investigated and remediated as soon as possible.
- Medium risk vulnerabilities indicate issues that could potentially result in information or system compromise.
- Low risk vulnerabilities indicate low severity problems or warnings, such as configurations that might reveal interesting reconnaissance information that could be used to facilitate a compromise.
- Informational risk vulnerabilities provide details about your systems that might be of interest but do not represent a security

Scan Summary

Scan Name	Scan Type	Total Targets	Active Hosts	Start Time	End Time	Total Time
PCI Scan	PCI Scan	1	1	2016-07-25 08:57:37	2016-07-25 10:03:40	1 hour, 5 minutes



Top 5 Vulnerabilities

Highest Risk Vulnerabilities	Severity	Count
.ida/idq ISAPI Mappings	Low	4
Auto-Completion Enabled for Password Fields	Low	3
No X-FRAME-OPTIONS Header	Low	2
Remote Desktop Protocol Service Supports SSL	Low	1
HTTP Responses Missing Character Encoding	Info	12