ManageEngine
Vulnerability Manager Plus

March 29,2023 10:40 PM

Computer Name	:	ALEXANDRGAN0B9F
Operating System	:	Windows Server 2019 Standard Edition (x64)
Service Pack	:	Windows Server 2019 (x64)
Language	:	NA
Health Status	:	UnKnown
Last Patched Time	:	--
Last Scan Status	:	Scanning Failed
IP Address	:	10.211.55.3
Domain	:	WORKGROUP
Remote Office	:	Local Office
Logged On Users	:	--
Last Successful Scan	:	--
Last Boot Time	:	Mar 29, 2023 11:18 PM
Reboot Required	:	No

Table of Contents

Resource-level Security Configurations

About

Provides an overview of the patches and vulnerabilities in a resource.

This report helps you ease the tension by providing you the list of patches, systems, vulnerabilities, misconfigurations and other threats that you have to act on immediately. The patch status summary provided you with the higher level view of the missing and installed patches in your network. Prioritize the missing patches using the severity split up graph. The next set of sections helps you understand about the health of the resource.

Resource Health Overview

Vulnerabilities

Vulnerability

No Data

System Misconfigurations

System Misconfiguration

No Data

Web Server Misconfiguration

Web Server Misconfiguration

No Data

Patches

Patch

No Data

ManageEngine
Vulnerability Manager Plus

3

Resource-level Vulnerabilities

Application Vulnerabilities

Vulnerabilities	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Updated Date	Supported Date	OS Platform
No data found.								

Web Server Vulnerabilities

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Updated Date	Supported Date
No data found.								

Database Server Vulnerabilities

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Updated Date	Supported Date
No data found.								

Content Management Systems

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Updated Date	Supported Date
No data found.								

Zero-day Vulnerabilities

Threats	Threat Category
No Results matching this criteria available	

Peer to peer

Software Name	Vendor
No Peer-To-Peer software found on the specified criteria	

Remote Desktop Sharing

Software Name	Vendor
No Remote Desktop software found on the specified criteria	

End of Life

Software Name	Vendor	Expiry Date	Days to Expire
No End-Of-Life software found on the specified criteria			

Excluded Vulnerabilities

Vulnerabilities	Exploit Status	Patch Availability	Reason for exclusion	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Updated Date	Supported Date
No Vulnerabilities are excluded								

Excluded Server Vulnerabilities

Vulnerabilities	Exploit Status	Patch Availability	Reason for exclusion	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Updated Date	Supported Date
No Vulnerabilities are excluded								

Excluded Risky Software

Software Name	Vendor	Reason for exclusion
No Applications are excluded		

Resource-level Patches

Missing Patches

Patch ID	Bulletin ID	Patch Description	Vendor	Patch Type	Approve Status	Remarks	Deployed Time	Patch Uninstallation
No Patches available								

Installed Patches

Patch ID	Bulletin ID	Patch Description	Vendor	Patch Type	Approve Status	Remarks	Deployed Time	Patch Uninstallation
No Patches available								

Declined Patches

Patch ID	Patch Status	Bulletin ID	Patch Description	Vendor	Patch Type	Patch Uninstallation
No Patches available						

Resource-level Security Configurations

System Misconfigurations

Misconfiguration	Category	Reboot Required
No security misconfigurations are detected on the specified criteria		

Web Server Misconfiguration

Web Server Misconfiguration	Category	File Path
No web server misconfigurations are detected on the specified criteria		

Excluded Misconfiguration

Misconfiguration	Category	Reason for exclusion
No Misconfigurations are excluded		

Excluded Hardening

Web Server Misconfiguration	Category	File Path	Reason for exclusion
No Web server misconfigurations are excluded			