tenable Security Center

Data Attack Surface - Critical and Exploitable Vulnerabilities Report

Generated on April 16, 2025 at 6:16 PM EDT

admin superna [securityadmin]
SUPERNA

Confidential: The following report contains sensitive security information about the organization’s IT infrastructure. Refer to your company’s policy regarding data classification and handling of sensitive information.

Table of Contents

About this Report

This report provides a summary of critical severity vulnerabilities. The report has an executive summary chapter showing tables and trend graphs highlighting the status of critical severity vulnerabilities. The two following chapters provide the delta between critical severity vulnerabilities that are exploitable versus not exploitable. This report will provide a summary of information for critical vulnerabilities with exploits associated with several tools that include: Metasploit, Core Impact, or CANVAS scripts. This report is meant to be used during individual scans or to be executed after a scan as a post-processing event. This template can be used to generate a report on all critical findings within your environment.

Executive Summary - This chapter provides a series of tables and charts to provide a summary view of critical vulnerabilities and the comparison to the exploitability of the vulnerability. The tables provide two views, one with vulnerabilities discovered over time in the last 30 days, and the other view of vulnerabilities to the exploit framework. The trend analysis provides a 6 month view of exploitable critical vulnerabilities and overall count of total critical vulnerabilities over the past 6 months.

Exploitable Vulnerability Summary - This chapter displays a summary of top exploitable critical vulnerabilities. The chapter contains a bar chart of the top 20 exploitable systems, a table of top 10 systems with system details, a port summary, and the top exploitable critical vulnerabilities.

Critical Vulnerability Summary - This chapter displays a summary of top critical vulnerabilities. The chapter contains a bar chart of the top 20 systems, a table of top 10 systems with system details, a port summary, and the top critical vulnerabilities.

Executive Summary

This chapter provides a series of tables and charts to provide a summary view of critical vulnerabilities and the comparison to the exploitability of the vulnerability. The tables provide two views, one with vulnerabilities discovered over time in the last 30 days, and the other view of vulnerabilities to the exploit framework. The trend analysis provides a 6 month view of exploitable critical vulnerabilities and overall count of total critical vulnerabilities over the past 6 months.

This table provides a summary of new exploitable vulnerabilities that have been discovered over the past 30 days, broken down into weekly increments. This table also includes a column for newly identified (never before seen) IP addresses by active and passive scanning, along with log analysis.

Current Vulnerabilities (Exploitable)

	New IP's	Info	Low	Medium	High	Critical
< 7 Days	0	0	0	0	0	0
8 - 14 Days	0	0	0	0	0	0
15 - 21 Days	0	0	0	0	0	0
22 - 30 Days	0	0	0	0	0	0

This table provides a summary of new vulnerabilities that have been discovered over the past 30 days, broken down into weekly increments. This table also includes a column for newly identified (never before seen) IP addresses by active and passive scanning, along with log analysis.

Current Vulnerabilities

	New IP's	Info	Low	Medium	High	Critical
< 7 Days	0	0	0	0	0	0
8 - 14 Days	0	0	0	0	0	0
15 - 21 Days	0	2	0	0	0	0
22 - 30 Days	0	1	0	0	0	0

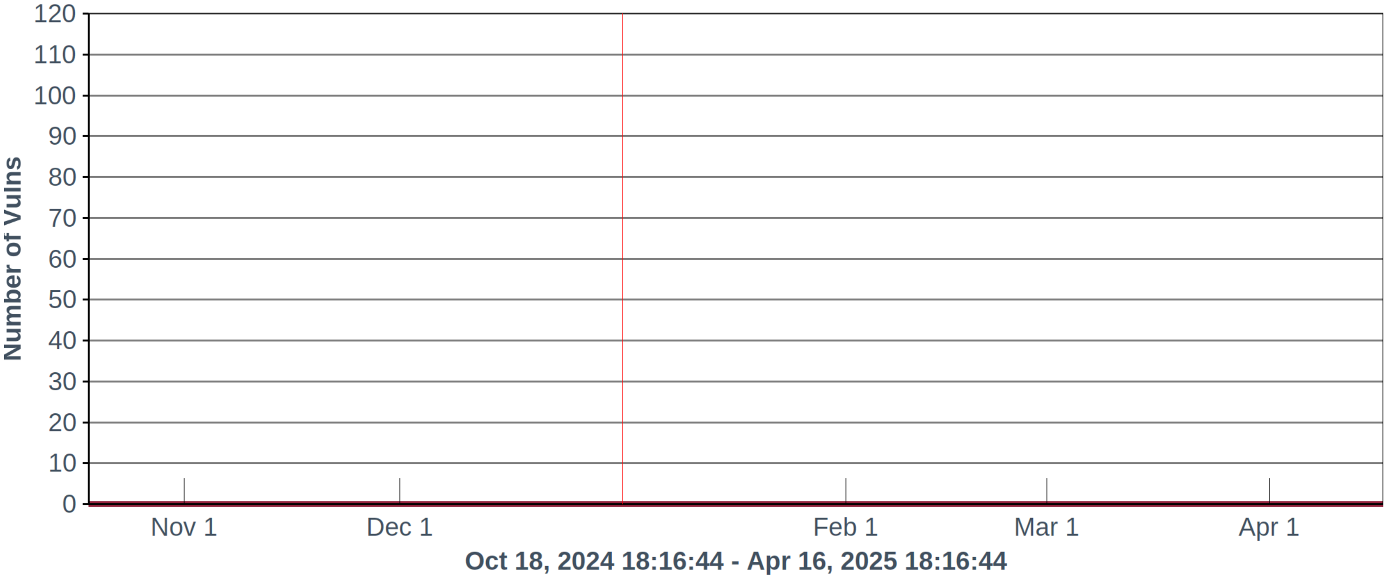
This table provides a matrix of exploitable vulnerabilities. There are 4 columns showing the total exploitable vulnerabilities, followed by columns for severity levels. The rows are organized by exploit framework, including the new tag “Exploitable by Malware”. The first row shows the count of exploitable vulnerabilities. The subsequent rows are broken down using the exploit frameworks. The cells show the vulnerability count of exploitable vulnerabilities for each framework based on severity. If 0 is present, then 0 vulnerabilities are identified and cell is green with white text. If 1 - 10 vulnerabilities are exploitable by a framework, the cell is white on yellow. If 11 – 50 vulnerabilities are exploitable by a framework, the cell is white on orange. If more than 51 vulnerabilities are exploitable by a framework, the cell is white on red.

Exploitable Matrix (Vulnerability Count)

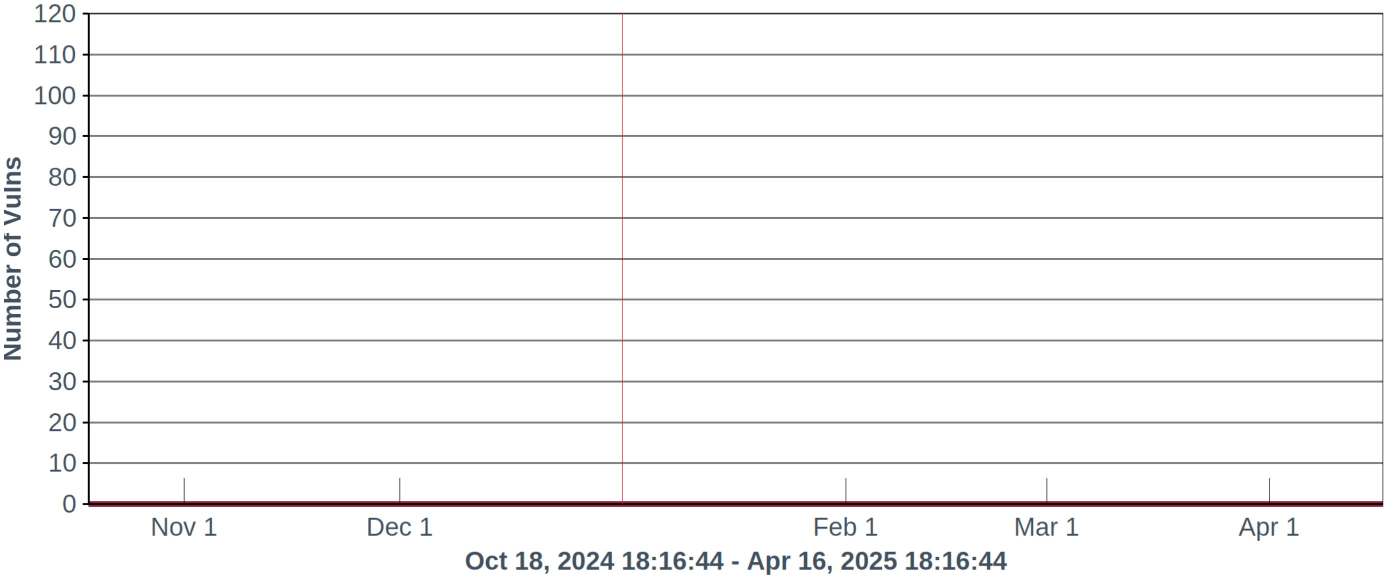
	Total	Medium	High	Critical
Exploitable	10	5	2	3
Malware	3	1	1	1
Core Impact	0	0	0	0
Canvas	1	1	0	0
Metasploit	0	0	0	0

These graphs show a historic view of vulnerabilities discovered on a monthly basis. The graphs analyze data over the past 6 months, taking data points every 15 days, and show new vulnerabilities for the preceding 15 days. From this, management can see the trend on vulnerability discovery. This method will show peaks in vulnerabilities as new events occur and when new scans are completed in SecurityCenter. The first graph is for critical vulnerabilities that are exploitable, while the second graph shows the total amount of critical vulnerabilities.

6 Month Trending Per Month (Exploitable)



6 Month Trending Per Month

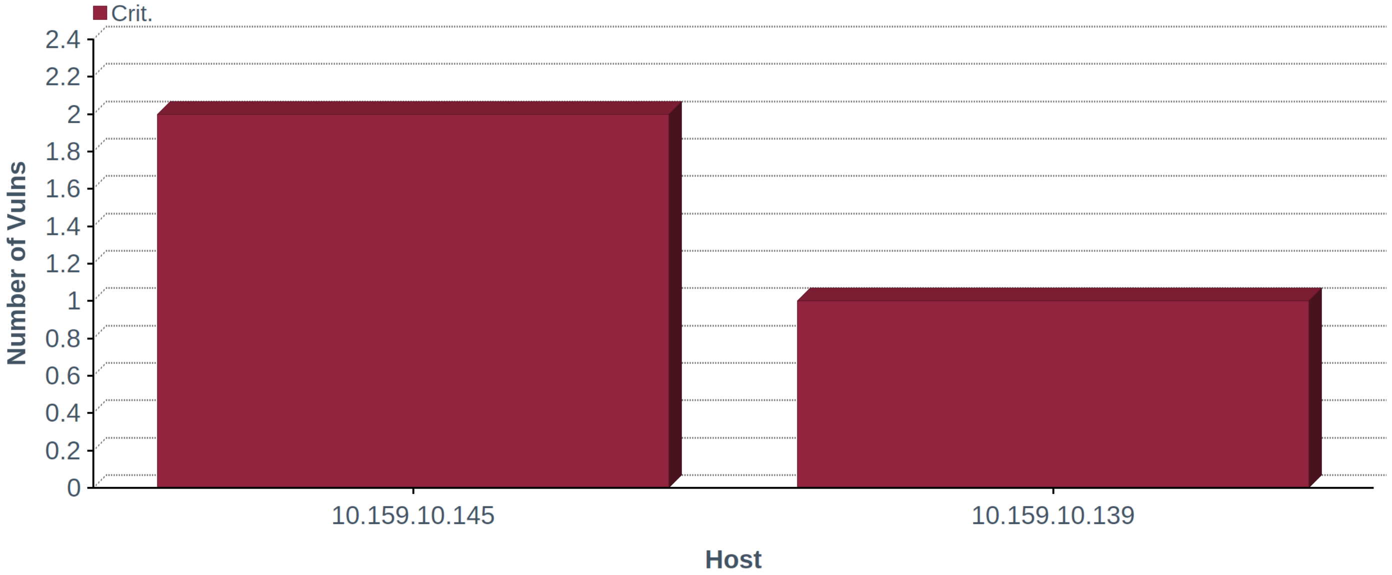


Exploitable Vulnerability Summary

This chapter displays a summary of top exploitable critical vulnerabilities. The chapter contains a bar chart of the top 20 exploitable systems, a table of top 10 systems with system details, a port summary, and the top exploitable critical vulnerabilities.

This chart displays the top 20 systems with critical vulnerabilities. The bar represents the number of exploitable vulnerabilities discovered on the system. These systems contain known exploitable vulnerabilities and should be patched as soon as possible.

Top 20 Critical Systems



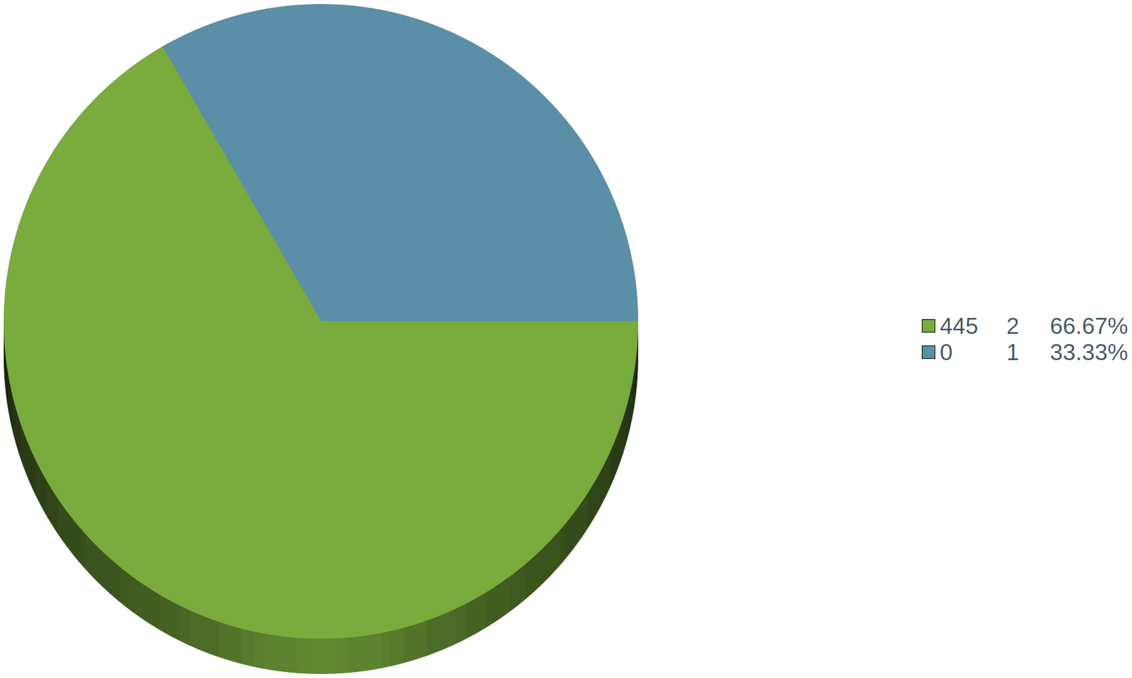
This table displays the top 10 systems with critical vulnerabilities. The bar represents the number of exploitable vulnerabilities discovered on the system. These systems contain known exploitable vulnerabilities and should be patched as soon as possible.

Top IP Findings

IP Address	NetBIOS Name	DNS Name	OS CPE	MAC Address	Crit.
10.159.10.145	addg1.test\DG-WIN145	DG-WIN145	cpe:/o:microsoft:windows_server_2019:10.0.17763.5936:-	00:50:56:b4:b2:27	2
10.159.10.139		dg-igls139	cpe:/o:opensuse:leap:15.5	00:50:56:b4:dc:04	1

This pie chart displays a summary of the top 10 ports used by exploitable vulnerabilities with a critical severity. The legend contains the port number and a count of occurrences, with a percentage for each discovered port.

Top 10 Ports



This table provides a detailed review of the top 20 critical severity vulnerabilities that are exploitable. The table contains the vulnerability name, plugin family, severity and number of occurrences.

Critical Vulnerabilities

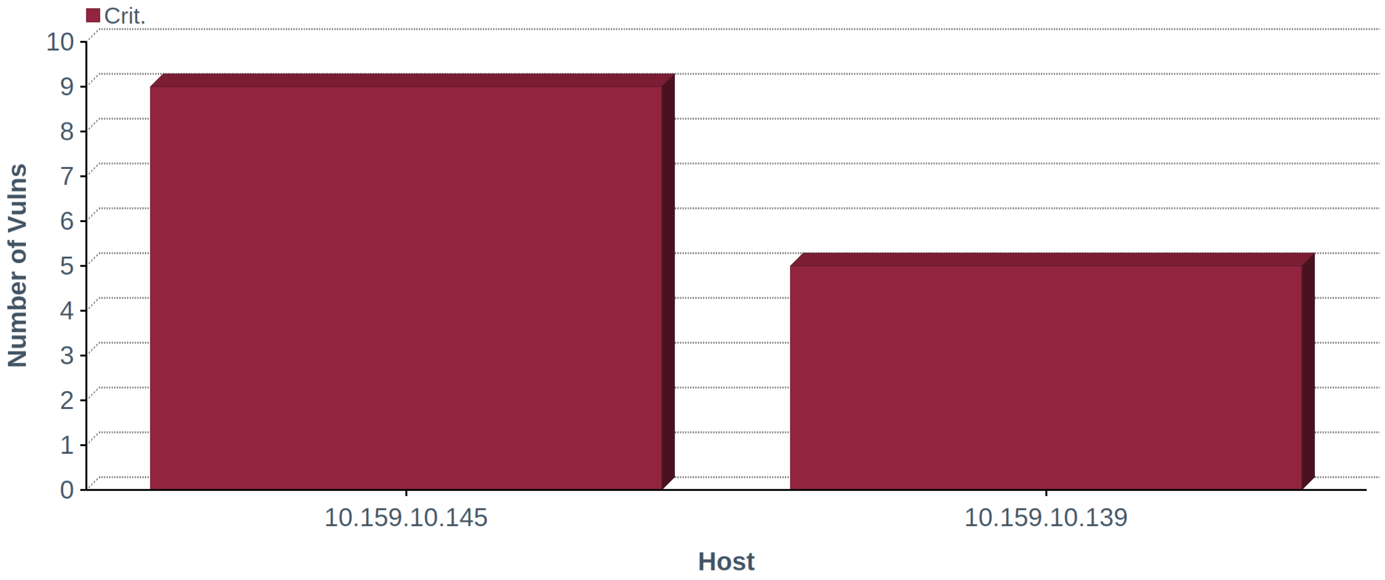
Plugin Name	Family	Severity	Total
KB5041578: Windows 10 version 1809 / Windows Server 2019 Security Update (August 2024)	Windows : Microsoft Bulletins	Critical	1
KB5040430: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2024)	Windows : Microsoft Bulletins	Critical	1
Apache Log4j 1.x Multiple Vulnerabilities	Misc.	Critical	1

Critical Vulnerability Summary

This chapter displays a summary of top critical vulnerabilities. The chapter contains a bar chart of the top 20 systems, a table of top 10 systems with system details, a port summary, and the top critical vulnerabilities.

This chart displays the top 20 systems with critical vulnerabilities. The bar represents the number of vulnerabilities discovered on the system. These systems contain known vulnerabilities and should be patched as soon as possible.

Top 20 Critical Systems



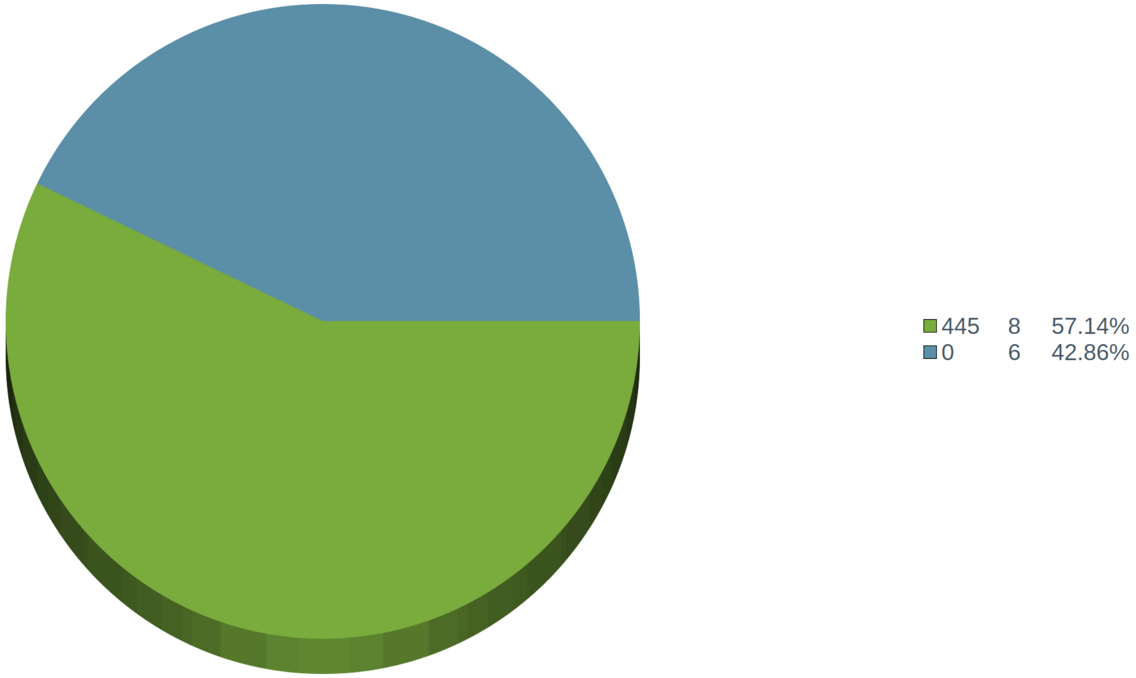
This table displays the top 10 systems with critical vulnerabilities. The bar represents the number of vulnerabilities discovered on the system. These systems contain known critical severity vulnerabilities and should be patched as soon as possible.

Top IP Findings

IP Address	NetBIOS Name	DNS Name	OS CPE	MAC Address	Crit.
10.159.10.145	addg1.test\DG-WIN145	DG-WIN145	cpe:/o:microsoft:windows_server_2019:10.0.17763.5936:-	00:50:56:b4:b2:27	9
10.159.10.139		dg-igls139	cpe:/o:opensuse:leap:15.5	00:50:56:b4:dc:04	5

This pie chart displays a summary of the top 10 ports used by vulnerabilities with a critical severity. The legend contains the port number and a count of occurrences, with a percentage for each discovered port.

Top Ports



This table provides a detailed review of the top 20 critical severity vulnerabilities. The table contains the vulnerability name, plugin family, severity and number of occurrences.

Critical Vulnerabilities

Plugin Name	Family	Severity	Total
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
NO NAME	N/A	Critical	1
KB5041578: Windows 10 version 1809 / Windows Server 2019 Security Update (August 2024)	Windows : Microsoft Bulletins	Critical	1
KB5040430: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2024)	Windows : Microsoft Bulletins	Critical	1
LibreOffice < 7.6.7 / 8.0.x < 24.2.3 (cve-2024-3044)	Misc.	Critical	1
Apache Log4j SEoL (<= 1.x)	Misc.	Critical	1
Apache Log4j 1.x Multiple Vulnerabilities	Misc.	Critical	1