

10.247.82.11

April 05, 2024

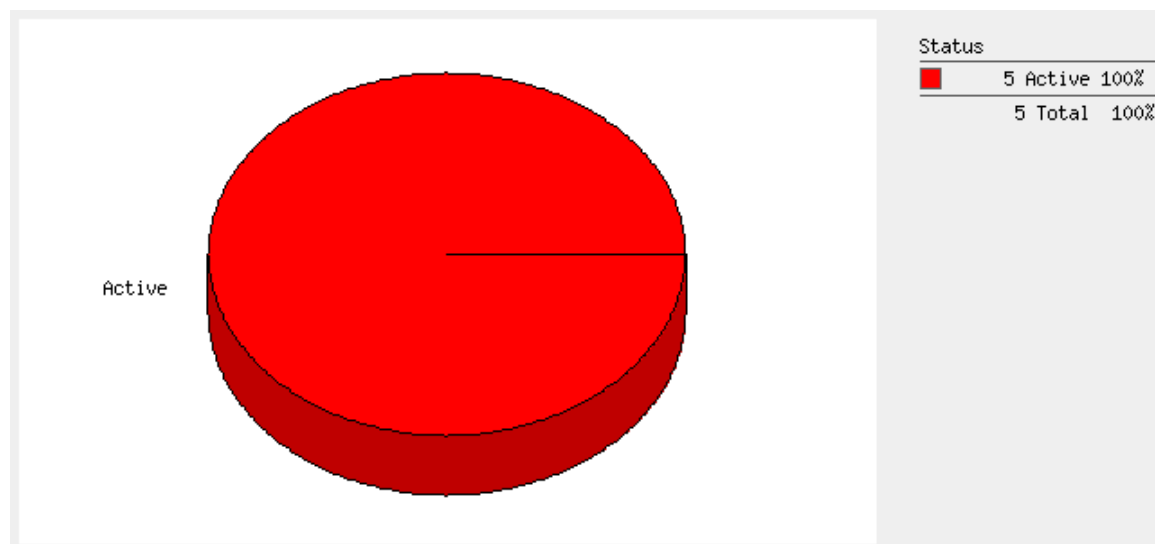
Report Summary	
User Name:	Alok Kumar Singh
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, 1st Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Delhi
Zip:	110053
Country:	India
Created:	05 Apr 2024 11:47:49 AM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.247.82.11
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 05 Apr 2024
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

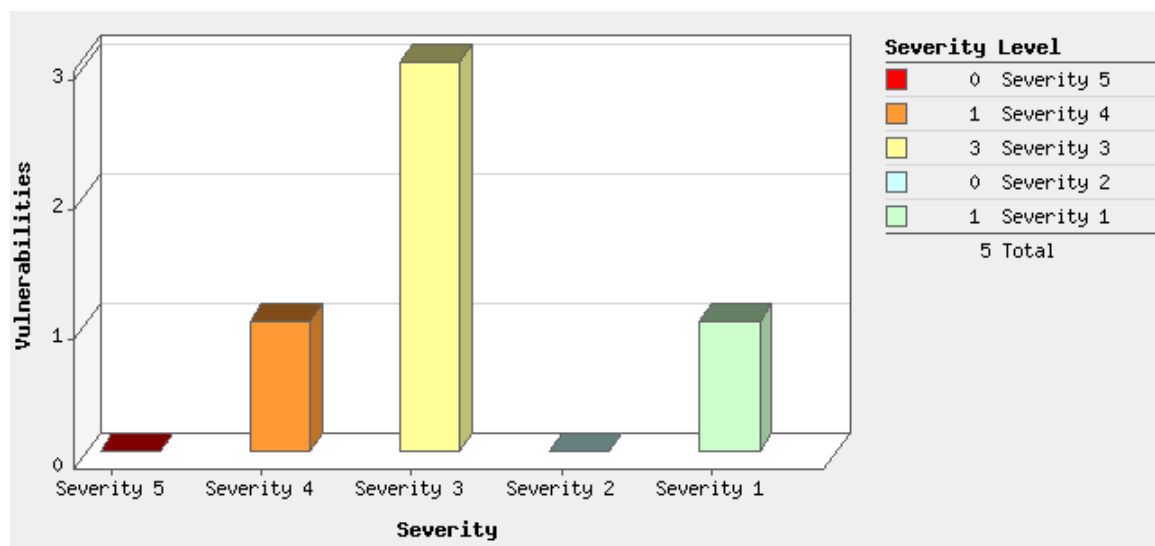
Vulnerabilities Total		5	Security Risk (Avg)		<div><div></div><div></div><div></div><div></div><div></div></div>	4.0	Business Risk		<div><div></div><div></div><div></div><div></div><div></div></div>	36/100
by Severity										
Severity	Confirmed		Potential		Information Gathered		Total			
5	0		-		-		0			
4	1		-		-		1			
3	3		-		-		3			
2	0		-		-		0			
1	1		-		-		1			
Total	5		-		-		5			

5 Biggest Categories								
Category	Confirmed		Potential		Information Gathered		Total	
RedHat	4		-		-		4	
Local	1		-		-		1	
Total	5		-		-		5	

Vulnerabilities by Status



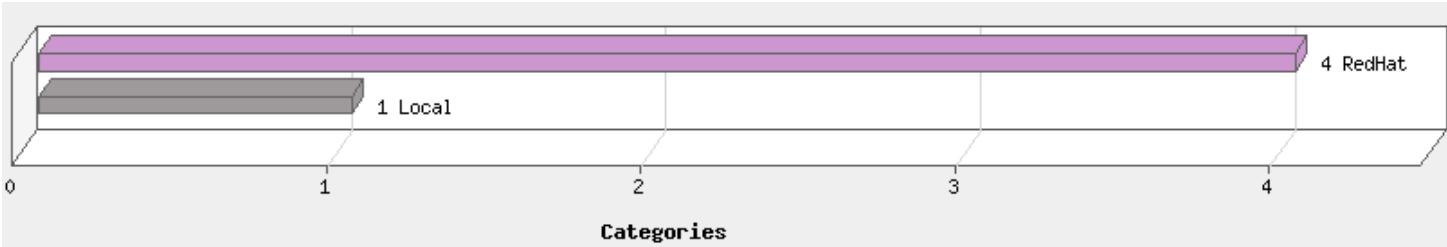
Vulnerabilities by Severity



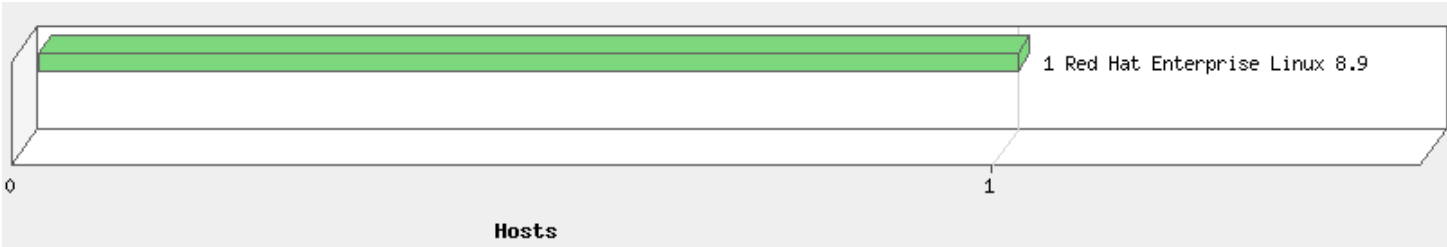
Information Gathered by Severity

There are no known vulnerabilities for this/these systems

Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.247.82.11 (hf71p-tpas123-001.spwh-lxcld.nic.in, -)

Red Hat Enterprise Linux 8.9

Host Identification Information	
IPs	
QG Host ID	00d1cb1e-ca49-4aee-99ba-fc7d3cda2af7

Vulnerabilities Total

5

Security Risk

4.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	1	-	-	1
3	3	-	-	3
2	0	-	-	0
1	1	-	-	1
Total	5	-	-	5

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
RedHat	4	-	-	4
Local	1	-	-	1
Total	5	-	-	5

Vulnerabilities (5)

4

Red Hat Update for kernel security (RHSA-2024:1607)

CVSS: 4.2

CVSS3.1: 7

Active

QID:

243160

CVSS Base:

5.4

[1]

Category:

RedHat

CVSS Temporal:

4.3

Associated CVEs:

CVE-2021-33631

,

CVE-2022-38096

,

CVE-2023-6546

,

CVE-2023-6931

,

CVE-2023-51042

,

CVE-2024-0565

,

CVE-2024-1086

Vendor Reference: [RHSA-2024:1607](#)
Bugtraq ID: -
Service Modified: 05 Apr 2024
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS3.1 Base: 7.8
CVSS3.1 Temporal: 7.0

First Detected: 04 Apr 2024 01:05:47 AM (GMT+0530)
Last Detected: 05 Apr 2024 06:56:18 AM (GMT+0530)
Times Detected: 7
Last Fixed: N/A

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

The kernel packages contain the linux kernel, the core of any linux operating system...Security Fix(es): kernel: vmwgfx: null pointer dereference in vmw_cmd_dx_define_query (cve-2022-38096). Kernel: out of boundary write in perf_read_group() as result of overflow a perf_event's read_size (cve-2023-6931). Kernel: gsm multiplexing race condition leads to privilege escalation (cve-2023-6546,zdi-can-20527). Kernel: cifs filesystem decryption improper input validation remote code execution vulnerability in function receive_encrypted_standard of client (cve-2024-0565). Kernel: use-after-free in amdgpu_cs_wait_all_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c (cve-2023-51042). Kernel: ext4: kernel bug in ext4_write_inline_data_end() (cve-2021-33631). Kernel: nf_tables: use-after-free vulnerability in the nft_verdict_init() function (cve-2024-1086). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for arm 64 8 aarch64. Red hat codeready linux builder for x86_64 8 x86_64. Red hat codeready linux builder for power, little endian 8 ppc64le. Red hat codeready linux builder for arm 64 8 aarch64.. Note: The preceding description block is extracted directly from the security advisory. Using automation, we have attempted to clean and format it as much as possible without introducing additional issues.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Refer to Red Hat security advisory RHSA-2024:1607 (<https://access.redhat.com/errata/RHSA-2024:1607>) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2024:1607: Red Hat Enterprise Linux (<https://access.redhat.com/errata/RHSA-2024:1607>)

RESULTS:

Package	Installed Version	Required Version
kernel-modules	4.18.0-425.3.1.el8.x86_64	4.18.0-513.24.1.el8_9
kernel-modules	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
kernel-modules	4.18.0-372.26.1.el8_6.x86_64	4.18.0-513.24.1.el8_9
python3-perf	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
kernel-core	4.18.0-372.26.1.el8_6.x86_64	4.18.0-513.24.1.el8_9
kernel-core	4.18.0-425.3.1.el8.x86_64	4.18.0-513.24.1.el8_9
kernel-core	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
kernel-tools	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
kernel-tools-libs	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
kernel-headers	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
bpftool	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9
kernel	4.18.0-425.3.1.el8.x86_64	4.18.0-513.24.1.el8_9
kernel	4.18.0-372.26.1.el8_6.x86_64	4.18.0-513.24.1.el8_9
kernel	4.18.0-513.18.1.el8_9.x86_64	4.18.0-513.24.1.el8_9

QID:

243155

Category:

RedHat

Associated CVEs:

[CVE-2023-28322](#), [CVE-2023-38546](#), [CVE-2023-46218](#)

Vendor Reference:

[RHSA-2024:1601](#)

Bugtraq ID:

-

Service Modified:

04 Apr 2024

User Modified:

-

Edited:

No

PCI Vuln:

Yes

Ticket State:

CVSS Base:

5.4

[\[1\]](#)

CVSS Temporal:

4.3

CVSS3.1 Base:

6.5

CVSS3.1 Temporal:

5.9

First Detected: 04 Apr 2024 01:05:47 AM (GMT+0530)
Last Detected: 05 Apr 2024 06:56:18 AM (GMT+0530)
Times Detected: 7
Last Fixed: N/A

CVSS Environment:

Asset Group:

-

Collateral Damage Potential:

-

Target Distribution:

-

Confidentiality Requirement:

-

Integrity Requirement:

-

Availability Requirement:

-

THREAT:

The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including http, ftp, and ldap...Security Fix(es): curl: information disclosure by exploiting a mixed case flaw (cve-2023-46218). Curl: more post-after-put confusion (cve-2023-28322). Curl: cookie injection with none file (cve-2023-38546). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for arm 64 8 aarch64.. Note: The preceding description block is extracted directly from the security advisory. Using automation, we have attempted to clean and format it as much as possible without introducing additional issues.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Refer to Red Hat security advisory RHSA-2024:1601 (<https://access.redhat.com/errata/RHSA-2024:1601>) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2024:1601: Red Hat Enterprise Linux (<https://access.redhat.com/errata/RHSA-2024:1601>)

RESULTS:

Package	Installed Version	Required Version
curl	7.61.1-33.el8.x86_64	7.61.1-33.el8_9.5
libcurl	7.61.1-33.el8.x86_64	7.61.1-33.el8_9.5
libcurl-devel	7.61.1-33.el8.x86_64	7.61.1-33.el8_9.5

QID:

243165

Category:

RedHat

Associated CVEs:

[CVE-2023-52425](#)

Vendor Reference:

[RHSA-2024:1615](#)

Bugtraq ID:

-

Service Modified:

03 Apr 2024

User Modified:

-

Edited:

No

PCI Vuln:

No

Ticket State:

CVSS Base:

5.4

[\[1\]](#)

CVSS Temporal:

4.3

CVSS3.1 Base:

7.5

CVSS3.1 Temporal:

6.7

First Detected: 04 Apr 2024 01:05:47 AM (GMT+0530)

Last Detected: 05 Apr 2024 06:56:18 AM (GMT+0530)

Times Detected: 7

Last Fixed: N/A

CVSS Environment:

- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

THREAT:

Expat is a c library for parsing xml documents...Security Fix(es): expat: parsing large tokens can trigger a denial of service (cve-2023-52425). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for arm 64 8 aarch64.. Note: The preceding description block is extracted directly from the security advisory. Using automation, we have attempted to clean and format it as much as possible without introducing additional issues.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Refer to Red Hat security advisory RHSA-2024:1615 (<https://access.redhat.com/errata/RHSA-2024:1615>) for updates and patch information.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

RHSA-2024:1615: Red Hat Enterprise Linux (<https://access.redhat.com/errata/RHSA-2024:1615>)

RESULTS:

Package	Installed Version	Required Version
expat-devel	2.2.5-11.el8.x86_64	2.2.5-11.el8_9.1
expat	2.2.5-11.el8.x86_64	2.2.5-11.el8_9.1



3 Red Hat Update for less (RHSA-2024:1610)

CVSS: 4 CVSS3.1: 7.5 Active

QID: 243159
Category: RedHat
Associated CVEs: [CVE-2022-48624](#)
Vendor Reference: [RHSA-2024:1610](#)
Bugtraq ID: -
Service Modified: 03 Apr 2024
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS Base: 5.4 [1]
CVSS Temporal: 4.0

CVSS3.1 Base: 8.6 [1]
CVSS3.1 Temporal: 7.5

First Detected: 04 Apr 2024 01:05:47 AM (GMT+0530)

Last Detected: 05 Apr 2024 06:56:18 AM (GMT+0530)

Times Detected: 7

Last Fixed: N/A

CVSS Environment:

- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

THREAT:

The "less" utility is a text file browser that resembles "more", but allows users to move backwards in the file as well as

forwards. Since "less" does not read the entire input file at startup, it also starts more quickly than ordinary text editors...Security Fix(es): less: missing quoting of shell metacharacters in lessclose handling (cve-2022-48624). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for arm 64 8 aarch64.. Note: The preceding description block is extracted directly from the security advisory. Using automation, we have attempted to clean and format it as much as possible without introducing additional issues.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Refer to Red Hat security advisory RHSA-2024:1610 (<https://access.redhat.com/errata/RHSA-2024:1610>) for updates and patch information.
Patch:

Following are links for downloading patches to fix the vulnerabilities:

RHSA-2024:1610: Red Hat Enterprise Linux (<https://access.redhat.com/errata/RHSA-2024:1610>)

RESULTS:

Package	Installed Version	Required Version
less	530-1.el8.x86_64	530-2.el8_9

 1 Shim package Multiple Vulnerabilities CVSS: 5.8 CVSS3.1: 7.6 Active

QID:	379359	CVSS Base:	6.8 [1]
Category:	Local	CVSS Temporal:	5.8
Associated CVEs:	CVE-2023-40547, CVE-2023-40546, CVE-2023-40548, CVE-2023-40549, CVE-2023-40550, CVE-2023-40551		
Vendor Reference:	CVE-2023-40547		
Bugtraq ID:	-		
Service Modified:	27 Mar 2024	CVSS3.1 Base:	8.3
User Modified:	15 Feb 2024	CVSS3.1 Temporal:	7.6
Edited:	Yes		
PCI Vuln:	Yes		
Ticket State:	Open		

First Detected: 10 Feb 2024 04:47:43 AM (GMT+0530)

Last Detected: 05 Apr 2024 06:56:18 AM (GMT+0530)

Times Detected: 229

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Shim is an open-source projects and other third parties built a small application, that contains the vendor certificate and code that verifies and runs the bootloader (typically GRUB2).

Shim is affected with multiple security vulnerabilities.

CVE-2023-40547 Remote code execution vulnerability was found in Shim

CVE-2023-40546 Fixes a LogError() invocation (NULL pointer dereference)

CVE-2023-40548 Fixes an integer overflow on SBAT section size on 32-bit systems (heap overflow)

CVE-2023-40549 Fixes an out-of-bounds read when loading a PE binary

CVE-2023-40550 Fixes an out-of-bounds read when trying to validate the SBAT information

CVE-2023-40551 Fix bounds check for MZ binaries

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could lead to remote code execution, crash, denial of service and exposure of sensitive data

SOLUTION:

NOTE: Vendor has not released any patch yet for the associated CVE.

Refer to Red hat security advisory CVE-2023-40547
(<https://access.redhat.com/security/cve/cve-2023-40547>) Debian security advisory CVE-2023-40547
(<https://security-tracker.debian.org/tracker/CVE-2023-40547>), Suse security advisory CVE-2023-40547
(<https://www.suse.com/security/cve/CVE-2023-40547.html>) for updates.

RESULTS:

Resolves: CVE-2022-28737
Related: CVE-2020-10713
Related: CVE-2020-14308
Related: CVE-2020-14309
Related: CVE-2020-14310
Related: CVE-2020-14311

Appendix






Report Filters

Excluded Vulnerability Lists:	Exclusion RHEL Mariadb (QID- 240255), OpenSSH Information Disclosure Vulnerability (Generic) _CVE-2020-14145
Excluded QIDs:	240255, 650035
Status:	New, Active, Re-Opened
Display non-running kernels:	Off
Exclude non-running kernels:	On
Exclude non-running services:	Off
Exclude QIDs not exploitable due to configuration:	Off
Vulnerabilities:	State:Active
Included Operating Systems:	All Operating Systems

Report Legend




Vulnerability Levels



A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels




A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

Severity	Level	Description
 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.

CONFIDENTIAL AND PROPRIETARY INFORMATION.

Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2024, Qualys, Inc.