10.247.139.197

January 10, 2023

Report Summary

User Name:	Harjeet Singh
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, Ist Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Uttar Pradesh
Zip:	110053
Country:	India
Created:	10 Jan 2023 09:47:00 AM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.247.139.197
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 10 Jan 2023
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	8	Security Risk (Avg)	🟥🟥🟥□□ 3.0	Business Risk	64/100

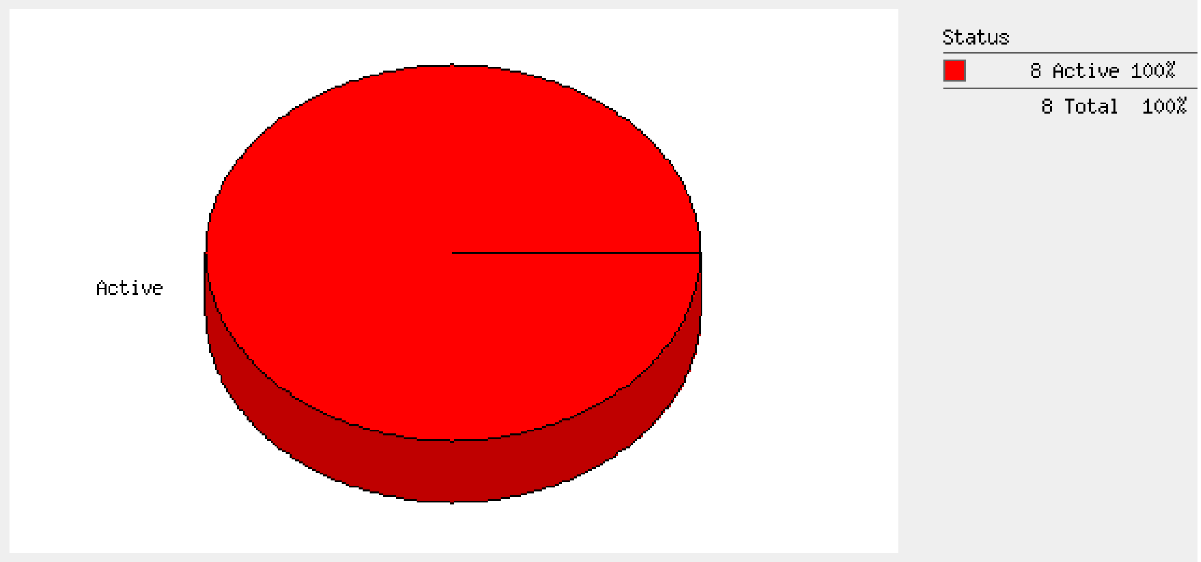
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	7	-	-	7
2	1	-	-	1
1	0	-	-	0
Total	8	-	-	8

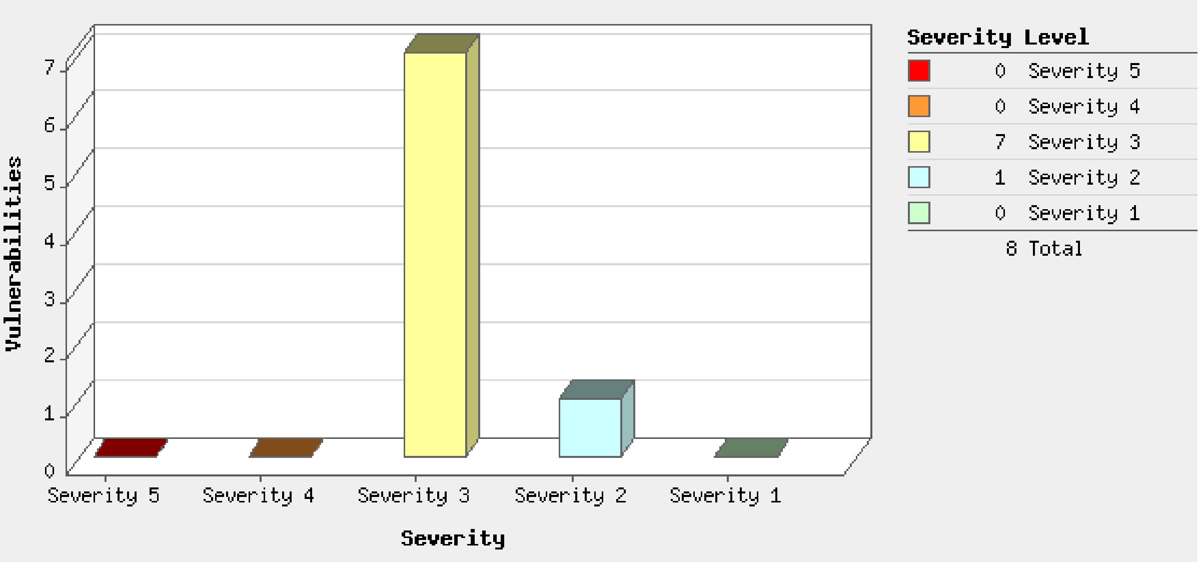
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Local	8	-	-	8
Total	8	-	-	8

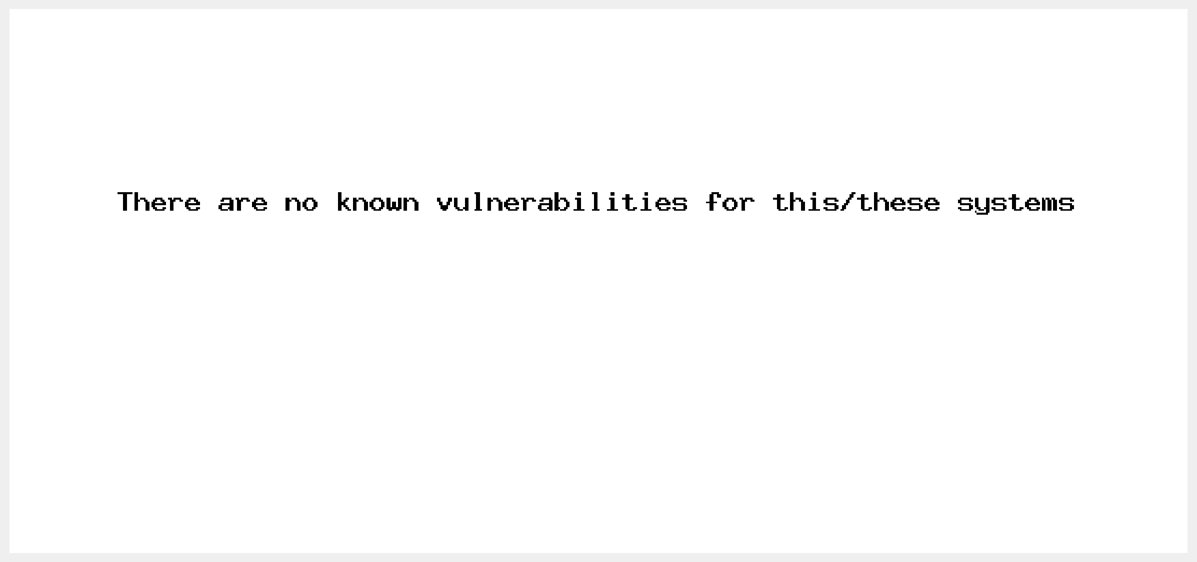
Vulnerabilities by Status



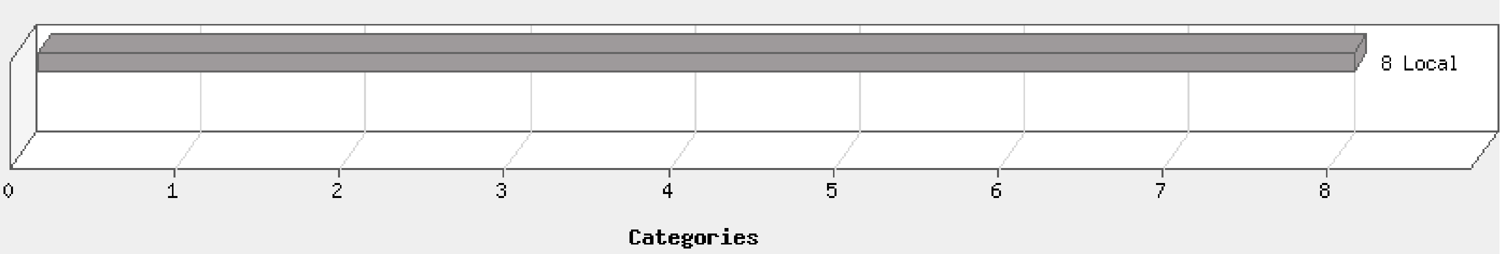
Vulnerabilities by Severity



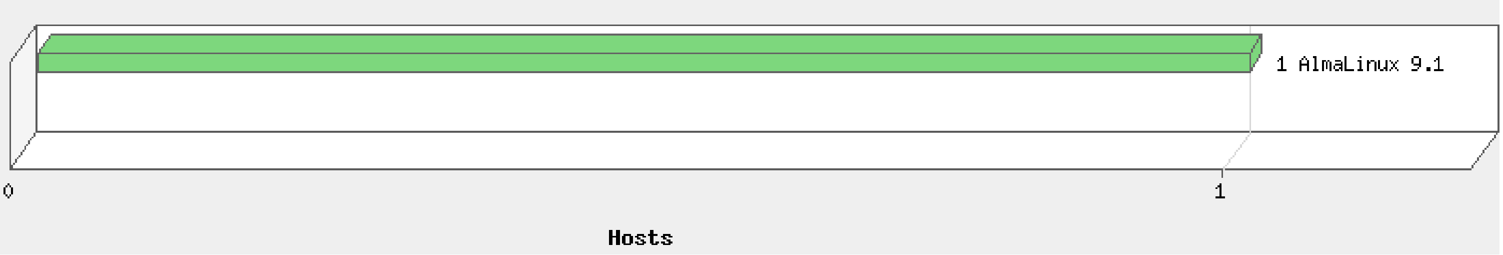
Information Gathered by Severity



Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.247.139.197 (tn73p-alma9tt-008, -) AlmaLinux 9.1

Host Identification Information	
IPs	
QG Host ID	7e787cea-8b5d-49ed-b226-bf7f54b3e96d

Vulnerabilities Total	8	Security Risk	🟥🟥🟥□□	3.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	7	-	-	7
2	1	-	-	1
1	0	-	-	0
Total	8	-	-	8

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Local	8	-	-	8
Total	8	-	-	8

Vulnerabilities (8)

🟥🟥🟥⬜⬜ 3 Linux Kernel RTL8169 NIC "RxMaxSize" Frame Size Remote Denial of Service Vulnerability CVSS: 6.3 CVSS3.1: - Active

QID:	116788	CVSS Base:	7.8
Category:	Local	CVSS Temporal:	6.3
Associated CVEs:	CVE-2009-4537		
Vendor Reference:	-		
Bugtraq ID:	37521 , 37521		
Service Modified:	04 May 2015	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

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. The following vulnerabilities were identified in the Linux kernel:
The Linux kernel is prone to a local denial-of-service vulnerability .
The following versions are vulnerable:
Linux kernel prior to 2.6.12
Linux Kernel 2.6.30 and later

IMPACT:
An attacker can exploit this issue to deny service to legitimate users. Other attacks are also possible.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULTS:

```
5.14.0-162.6.1.el9_1.x86_64
```

🟥🟥🟥⬜⬜ 3 Linux Kernel Multiple Vulnerabilities CVSS: 1.7 CVSS3.1: - Active

QID:	119077	CVSS Base:	2.1
Category:	Local	CVSS Temporal:	1.7
Associated CVEs:	CVE-2010-3849, CVE-2010-3850		
Vendor Reference:	Linux Kernel		
Bugtraq ID:	-		
Service Modified:	20 Dec 2022	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The kernel packages form the core of the Linux operating system and are responsible for handling the basic functions of the operating system.
Multiple vulnerabilities exists in Linux Kernel caused by:-
1. The econet_sendmsg function in net/econet/af_econet.c in the Linux kernel and
2. The ec_dev_ioctl function in net/econet/af_econet.c in the Linux kernel
The vulnerabilities are reported in all the Linux Kernel versions before 2.6.36.2.

IMPACT:

Successful exploitation allows local users to bypass intended access restrictions and cause a denial of service.

SOLUTION:

Update to version 2.6.36.2 to resolve the issue. Refer to The Linux Kernel Archives (http://www.kernel.org/) to obtain additional details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Linux kernel: Linux (Linux 2.6.36.2) (http://www.kernel.org/)

RESULTS:

```
Linux tn73p-alma9tt-008 5.14.0-162.6.1.el9_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 15 07:49:10 EST 2022 x86_64 x86_64 x86_64 GNU/
Linux
```

🟥🟥🟥□□ 3 Linux Kernel Information Disclosure Vulnerability CVSS: 1.6 CVSS3.1: - Active

QID:	116239	CVSS Base:	2.1
Category:	Local	CVSS Temporal:	1.6
Associated CVEs:	CVE-2009-0676		
Vendor Reference:	-		
Bugtraq ID:	33846		
Service Modified:	02 Jul 2010	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The kernel packages form the core of the Linux operating system and are responsible for handling the basic functions of the operating system.
Linux kernel is prone to the following vulnerabilities:
- An information disclosure vulnerability exists in "virt_to_page()" function of the kernel that is caused when the skb->data buffer is reused by SLAB before the send side socket actually gets the TX packet out to the device.
- A security weakness exists in the kernel that is caused due to a logic error within the "skfp_ioctl()" function in drivers/net/skfp/skfddi.c, which can be exploited to reset the driver statistics without having CAP_NET_ADMIN capabilities.
Linux kernel versions prior to 2.6.27.18 and 2.6.28.6 are affected.

IMPACT:

If this vulnerability is successfully exploited, it will allow attackers to view portions of kernel memory and bypass certain security restrictions.

SOLUTION:

To resolve this vulnerability, upgrade to the latest packages which contain a patch. These are available from the Linux Kernel Web site (http://kernel.org/).
Refer to Linux kernel advisory Linux 2.6.27.18 (http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27.18) and Linux 2.6.28.6 (http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.28.6) to address this issue and obtain further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Linux Kernel: Linux (kernel) (http://kernel.org/)

RESULTS:

```
Linux tn73p-alma9tt-008 5.14.0-162.6.1.el9_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 15 07:49:10 EST 2022 x86_64 x86_64 x86_64 GNU/Linux
```

■■■□□ 3 Linux Kernel "ebtables" Security Bypass Vulnerability CVSS: 1.6 CVSS3.1: - Active

QID:	116795	CVSS Base:	2.1
Category:	Local	CVSS Temporal:	1.6
Associated CVEs:	CVE-2010-0007		
Vendor Reference:	-		
Bugtraq ID:	37762		
Service Modified:	06 Apr 2010	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The kernel packages form the core of the Linux operating system and are responsible for handling the basic functions of the operating system.
The Linux kernel is prone to a security-bypass vulnerability.
Versions prior to Linux kernel 2.6.33-rc4 are affected.

IMPACT:

Local attackers can exploit this issue to bypass certain security restrictions and set or modify "ebtables" rules.

SOLUTION:

The vendor has released a fix in the GIT repository. Refer to GIT Repository link (http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=dce766af541f6605fa9889892c0280bab31c66ab) to obtain additional details.

RESULTS:

5.14.0-162.6.1.el9_1.x86_64

■■■□□ 3 Linux Kernel "/ipc/shm.c" Local Denial of Service Vulnerability CVSS: 3.7 CVSS3.1: - Active

QID:	116274	CVSS Base:	4.7
Category:	Local	CVSS Temporal:	3.7
Associated CVEs:	CVE-2009-0859		
Vendor Reference:	-		
Bugtraq ID:	34020		
Service Modified:	11 Nov 2019	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The kernel packages form the core of the Linux operating system and are responsible for handling the basic functions of the operating system.
The Linux kernel is prone to a local denial of service vulnerability that is caused because the "shm_get_stat()" function in the "/ipc/shm.c" source file makes an incorrect assumption about the type of inode parameter. This issue can be exploited by invoking the "ipcs" command on kernels configured with "!CONFIG_SHMEM".
Linux kernel Versions prior to 2.6.28.5 are affected.

IMPACT:

Attackers can exploit this issue to cause the Linux kernel to lock up, resulting in denial of service.

SOLUTION:

To resolve this vulnerability, upgrade to the latest packages which contain a patch. These are available from the Linux Kernel Web site (http://kernel.org/).
Refer to Linux kernel advisory Linux 2.6.28.5 (http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.28.5) to address this issue and obtain further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2009-0859 (https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=a68e61e8ff2d46327a37b69056998b47745db6fa)

RESULTS:

Linux tn73p-alma9tt-008 5.14.0-162.6.1.el9_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 15 07:49:10 EST 2022 x86_64 x86_64 x86_64 GNU/Linux

■■■□□ 3 Linux Kernel Multiple Security Vulnerabilities CVSS: 1.6 CVSS3.1: - Active

QID:	115337	CVSS Base:	2.1
Category:	Local	CVSS Temporal:	1.6

Associated CVEs:	CVE-2006-0555, CVE-2006-0741		
Vendor Reference:	-		
Bugtraq ID:	16925, 16922		
Service Modified:	05 Jun 2009	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

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

THREAT:
Linux kernel is prone to multiple vulnerabilities.
The following specific issues were identified:
a. Linux kernel NFS client is prone to a local denial of service vulnerability. This issue exists because the NFS client does not properly handle direct I/O with excessive O_DIRECT data.
b. Linux kernel is prone to a denial of service vulnerability when opening malformed ELF files with a bad entry address. This issue only occurs on Intel EM64T processors. Opening the malformed file will cause an endless recursive loop that causes the system to stop responding.
(Note: The CPU Type can be verified by typing "uname -m" on the Unix prompt. If it isn't "EM64T" you're not vulnerable to this issue.)

IMPACT:
An unprivileged local user could exploit this vulnerability to cause the NFS client to panic and crash.

SOLUTION:
Linux kernel patch 2.6.15-5 (http://www.kernel.org) has been released to fix this issue.

RESULTS:

```
Linux tn73p-alma9tt-008 5.14.0-162.6.1.el9_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 15 07:49:10 EST 2022 x86_64 x86_64 x86_64 GNU/
Linux
```

🟥🟥🟥□□ 3 Linux Kernel 32bit/64bit System Call Security Bypass Weaknesses CVSS: 2.8 CVSS3.1: - Active

QID:	116253	CVSS Base:	3.6
Category:	Local	CVSS Temporal:	2.8
Associated CVEs:	CVE-2009-0834, CVE-2009-0835		
Vendor Reference:	-		
Bugtraq ID:	33948, 33951		
Service Modified:	11 Nov 2019	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-

Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

The kernel packages form the core of the Linux operating system and are responsible for handling the basic functions of the operating system.
The following vulnerabilities were reported in the Linux kernel:
The Linux kernel has a built-in syscall filtering technology called "seccomp" which permits a process to restrict itself to an extremely restricted set of syscalls -- read(), write(), exit(), sigreturn(). An implementation error within the "PR_SET_SECCOMP" feature can be exploited to invoke restricted system calls. This issue occurs when 32-bit processes switch to 64-bit mode, or when 64-bit processes make 32-bit system calls. In both cases, seccomp restricts system calls based on the system call table associated with the process, rather than the table appropriate to the call being made.
An implementation error within the "audit_syscall_entry()" function can be exploited to bypass audit mechanisms imposed on system calls when 32-bit processes switch to 64-bit mode, or when 64-bit processes make 32-bit system calls.

IMPACT:

If this vulnerability is successfully exploited, it will allow a local attacker to bypass access control restrictions and make unintended system calls, which may result in an elevation of privileges.

SOLUTION:

An update is available to fix this issue in the Red Hat GIT repository. Refer to 487255 (https://bugzilla.redhat.com/show_bug.cgi?id=487255) for a list of proposed patches for upstream kernel.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Linux Kernel (https://bugzilla.redhat.com/show_bug.cgi?id=487255)

RESULTS:

```
Linux tn73p-alma9tt-008 5.14.0-162.6.1.el9_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 15 07:49:10 EST 2022 x86_64 x86_64 x86_64 GNU/
Linux
```

🟥🟥□□□ 2 Linux Kernel Security Key Functions Local Copy_To_User Race Vulnerability CVSS: 4.7 CVSS3.1: - Active

QID:	115344	CVSS Base:	7.1
Category:	Local	CVSS Temporal:	4.7
Associated CVEs:	CVE-2006-0457		
Vendor Reference:	-		
Bugtraq ID:	17084		
Service Modified:	16 Jun 2009	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 09 Jan 2023 10:10:59 PM (GMT+0530)

Last Detected: 10 Jan 2023 08:20:26 AM (GMT+0530)

Times Detected: 3

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The Linux kernel contains a keyring module that is designed to allow for the storage and maintenance of local key data for operations such as storing Kerberos credentials.
The kernel is vulnerable to a vulnerability in its security key functionality due to a local race condition that allows attackers to modify an argument of a copy operation after is has been validated, but prior to its use.
Specifically, there is a race condition between the time that the source argument of a "copy_to_user()" function is validated, and when the actual "copy_to_user()" function is called. This window of opportunity allows attackers to modify the trailing NULL byte of the string that is being copied into kernel memory.

IMPACT:

This vulnerability allows local attackers to crash the kernel, denying service to legitimate users. It may also be possible to read portions of kernel memory, allowing attackers to gain access to potentially sensitive information. This may aid them in further attacks.

SOLUTION:

Linux kernel patch 2.6.15-4 (http://www.kernel.org) has been released to fix this issue.

RESULTS:

```
Linux tn73p-alma9tt-008 5.14.0-162.6.1.el9_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 15 07:49:10 EST 2022 x86_64 x86_64 x86_64 GNU/
Linux
```

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.

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 2023, Qualys, Inc.