Qualys. Cloud Platform

National Informatics Centre

10.247.48.100

July 19, 2023

Report Summary	
User Name:	Rahul Tyagi
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, Ist Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Delhi
Zip:	110053
Country:	India
Created:	19 Jul 2023 09:46:35 AM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.247.48.100
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 19 Jul 2023
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	56	Security Risk (Avg)	4.0	Business Risk	36/100

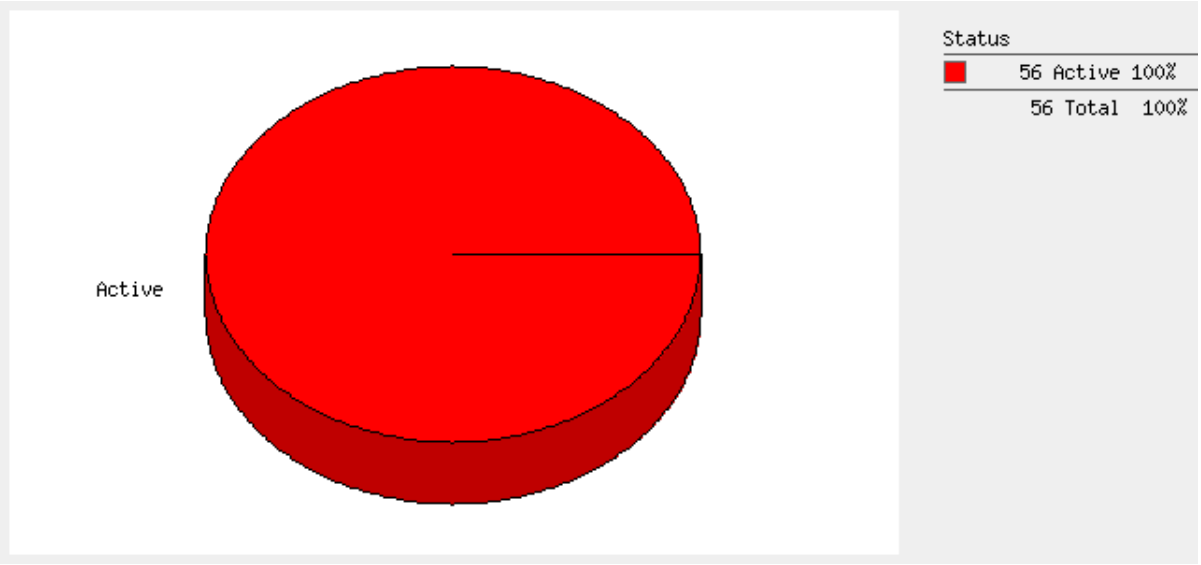
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	28	-	-	28
3	23	-	-	23
2	4	-	-	4
1	1	-	-	1
Total	56	-	-	56

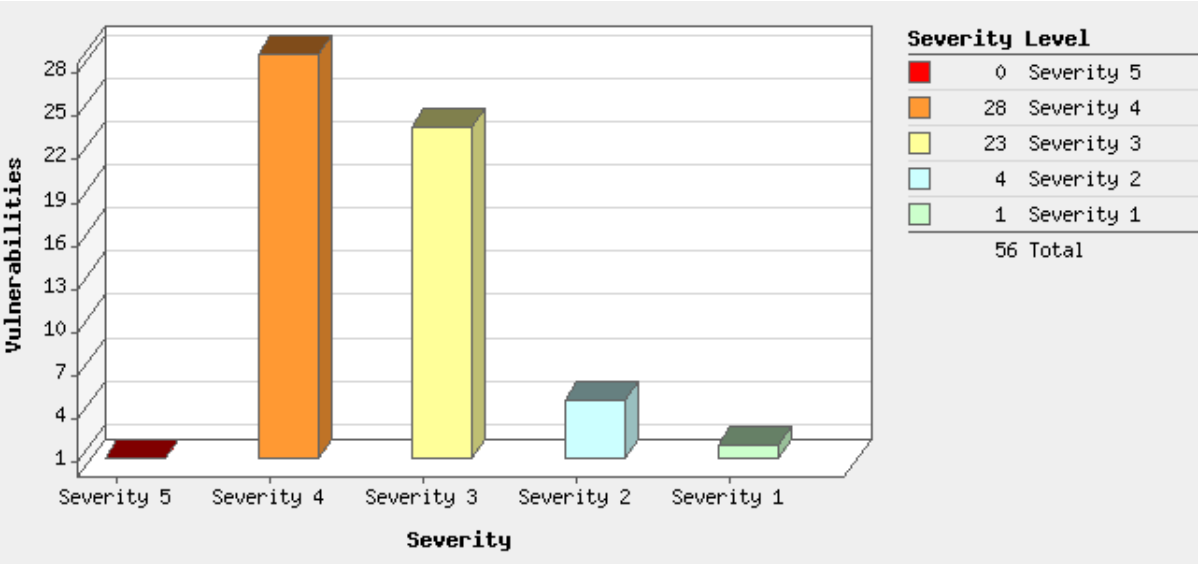
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
RedHat	55	-	-	55
Security Policy	1	-	-	1
Total	56	-	-	56

Vulnerabilities by Status



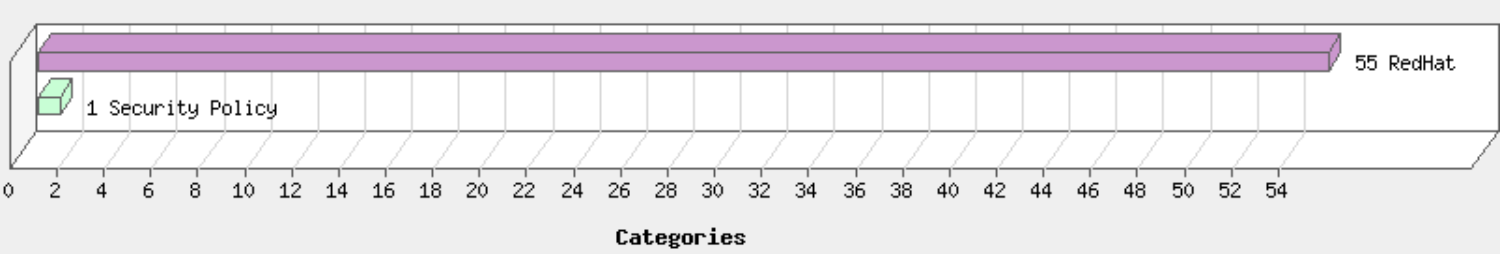
Vulnerabilities by Severity



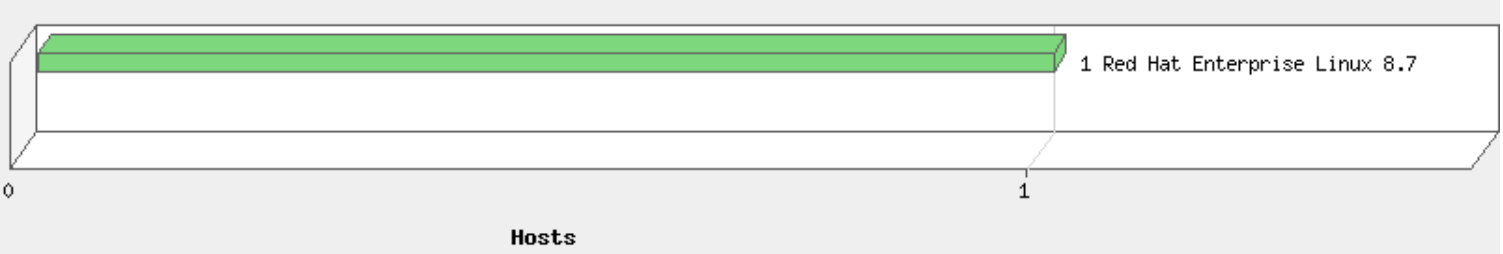
Information Gathered by Severity

There are no known vulnerabilities for this/these systems

Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.247.48.100 (dee1modp-websrv, -) Red Hat Enterprise Linux 8.7

Host Identification Information	
IPs	
QG Host ID	9db80698-284e-43e0-a07a-2b6075f70405

Vulnerabilities Total	56	Security Risk	4.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	28	-	-	28
3	23	-	-	23
2	4	-	-	4
1	1	-	-	1
Total	56	-	-	56

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
RedHat	55	-	-	55
Security Policy	1	-	-	1
Total	56	-	-	56

Vulnerabilities (56)

4 Red Hat Update for webkit2gtk3 (RHSA-2023:3108) CVSS: 4 CVSS3.1: 7.7 Active

QID:	241492	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-2203		
Vendor Reference:	RHSA-2023:3108		
Bugtraq ID:	-		
Service Modified:	26 May 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Webkitgtk is the port of the portable web rendering engine webkit to the gtk platform...Security Fix(es): webkitgtk: regression of cve-2023-28205 fixes in the Red Hat enterprise linux (cve-2023-2203). 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-2023:3108 (https://access.redhat.com/errata/RHSA-2023:3108) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3108: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3108)

RESULTS:

Package	Installed Version	Required Version
webkit2gtk3	2.36.7-1.el8_7.1.x86_64	2.38.5-1.el8_8.3

webkit2gtk3-jsc	2.36.7-1.el8_7.1.x86_64	2.38.5-1.el8_8.3

4 Red Hat Update for webkit2gtk3 (RHSA-2023:1919)

CVSS: 4.5 CVSS3.1: 8.2 Active

QID:	241373	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.5
Associated CVEs:	CVE-2023-28205		
Vendor Reference:	RHSA-2023:1919		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	8.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 25 Apr 2023 03:49:45 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 235

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Webkitgtk is the port of the portable web rendering engine webkit to the gtk platform...Security Fix(es): webkitgtk: use-after-free leads to arbitrary code execution (cve-2023-28205). 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-2023:1919 (https://access.redhat.com/errata/RHSA-2023:1919) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1919: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1919)

RESULTS:

Package	Installed Version	Required Version
webkit2gtk3	2.36.7-1.el8_7.1.x86_64	2.36.7-1.el8_7.3
webkit2gtk3-jsc	2.36.7-1.el8_7.1.x86_64	2.36.7-1.el8_7.3

4 Red Hat Update for firefox (RHSA-2023:0808)

CVSS: 4 CVSS3.1: 7.7 Active

QID:	241192	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-0767, CVE-2023-25728, CVE-2023-25729, CVE-2023-25730, CVE-2023-25732, CVE-2023-25735, CVE-2023-25737, CVE-2023-25739, CVE-2023-25742, CVE-2023-25743, CVE-2023-25744, CVE-2023-25746		
Vendor Reference:	RHSA-2023:0808		
Bugtraq ID:	-		
Service Modified:	09 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		

PCI Vuln: Yes
Ticket State:

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 373
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Mozilla firefox is an open-source web browser, designed for standards compliance, performance, and portability...Security Fix(es): mozilla: arbitrary memory write via pkcs 12 in nss (cve-2023-0767). Mozilla: content security policy leak in violation reports using iframes (cve-2023-25728). Mozilla: screen hijack via browser fullscreen mode (cve-2023-25730). Mozilla: potential use-after-free from compartment mismatch in spidermonkey (cve-2023-25735). Mozilla: invalid downcast in svgutils::setupstrokegeometry (cve-2023-25737). Mozilla: use-after-free in mozilla::dom::scriptloadcontext::~scriptloadcontext (cve-2023-25739). Mozilla: fullscreen notification not shown in firefox focus (cve-2023-25743). Mozilla: memory safety bugs fixed in firefox 110 and firefox esr 102.8 (cve-2023-25744). Mozilla: memory safety bugs fixed in firefox esr 102.8 (cve-2023-25746). Mozilla: extensions could have opened external schemes without user knowledge (cve-2023-25729). Mozilla: out of bounds memory write from encodeinputstream (cve-2023-25732). Mozilla: web crypto importkey crashes tab (cve-2023-25742). 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-2023:0808 (https://access.redhat.com/errata/RHSA-2023:0808) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0808: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0808)

RESULTS:

Package	Installed Version	Required Version
firefox	102.6.0-1.el8_7.x86_64	102.8.0-2.el8_7

4 Red Hat Update for tar (RHSA-2023:0842) CVSS: 4.2 CVSS3.1: 5 Active

QID:	241201	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-48303		
Vendor Reference:	RHSA-2023:0842		
Bugtraq ID:	-		
Service Modified:	31 May 2023	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.0
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 373
Last Fixed: N/A

CVSS Environment:

Asset Group:	-

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

THREAT:
The gnu tar program can save multiple files in an archive and restore files from an archive...Security Fix(es): tar: heap buffer overflow at from_header() in list.c via specially crafted checksum (cve-2022-48303). 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-2023:0842 (https://access.redhat.com/errata/RHSA-2023:0842) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0842: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0842)

RESULTS:

Package	Installed Version	Required Version
tar	1.30-6.el8.x86_64	1.30-6.el8_7.1

4 Red Hat Update for sudo (RHSA-2023:0284)

CVSS: 4.2 CVSS3.1: 7 Active

QID:	241081	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2023-22809		
Vendor Reference:	RHSA-2023:0284		
Bugtraq ID:	-		
Service Modified:	14 Jul 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 373
Last Fixed: N/A

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

THREAT:
The sudo packages contain the sudo utility which allows system administrators to provide certain users with the permission to execute privileged commands, which are used for system management purposes, without having to log in as root...Security Fix(es): sudo: arbitrary file write with privileges of the runas user (cve-2023-22809). 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-2023:0284 (https://access.redhat.com/errata/RHSA-2023:0284) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0284: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0284)

RESULTS:

Package	Installed Version	Required Version
sudo	1.8.29-8.el8.x86_64	1.8.29-8.el8_7.1

4 Red Hat Update for libxpm (RHSA-2023:0379)

CVSS: 4.2 CVSS3.1: 7.9 Active

QID:	241116	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-4883, CVE-2022-44617, CVE-2022-46285		
Vendor Reference:	RHSA-2023:0379		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

Last Fixed: N/A

CVSS Environment:

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

THREAT:
X.org x11 libxpm runtime library...Security Fix(es): libxpm: compression commands depend on $path (cve-2022-4883). Libxpm: runaway loop on width of 0 and enormous height (cve-2022-44617). Libxpm: infinite loop on unclosed comments (cve-2022-46285). 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-2023:0379 (https://access.redhat.com/errata/RHSA-2023:0379) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0379: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0379)

RESULTS:

Package	Installed Version	Required Version
libXpm	3.5.12-8.el8.x86_64	3.5.12-9.el8_7

4 Red Hat Update for c-ares (RHSA-2023:3584)

CVSS: 4 CVSS3.1: 6.5 Active

QID:	241710	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-32067		

Vendor Reference: RHSA-2023:3584
Bugtraq ID: -
Service Modified: 15 Jun 2023
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

CVSS3.1 Base: 7.5
CVSS3.1 Temporal: 6.5

First Detected: 16 Jun 2023 09:25:50 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 80
Last Fixed: N/A

CVSS Environment:

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

THREAT:
The c-ares c library defines asynchronous dns (domain name system) requests and provides name resolving api...Security Fix(es): c-ares: 0-byte udp payload denial of service (cve-2023-32067). <H2></H2> Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3584 (https://access.redhat.com/errata/RHSA-2023:3584) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3584: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3584)

RESULTS:

Package	Installed Version	Required Version
c-ares	1.13.0-6.el8.x86_64	1.13.0-6.el8_8.2

4 Red Hat Update for python3 (RHSA-2023:3591) CVSS: 4.2 CVSS3.1: 6.7 Active

QID: 241718
Category: RedHat
Associated CVEs: CVE-2023-24329
Vendor Reference: RHSA-2023:3591
Bugtraq ID: -
Service Modified: 16 Jun 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS Base: 5.4 [1]
CVSS Temporal: 4.3

CVSS3.1 Base: 7.5
CVSS3.1 Temporal: 6.7

First Detected: 16 Jun 2023 09:25:50 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 80
Last Fixed: N/A

CVSS Environment:

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

THREAT:

Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems...Security Fix(es): python: urllib.parse url blocklisting bypass (cve-2023-24329). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3591 (https://access.redhat.com/errata/RHSA-2023:3591) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3591: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3591)

RESULTS:

Package	Installed Version	Required Version
python3-libs	3.6.8-48.el8_7.x86_64	3.6.8-51.el8_8.1
platform-python	3.6.8-48.el8_7.x86_64	3.6.8-51.el8_8.1

4 Red Hat Update for firefox (RHSA-2023:1336)

CVSS: 4 CVSS3.1: 7.7 Active

QID:	241272	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-25751, CVE-2023-25752, CVE-2023-28162, CVE-2023-28164, CVE-2023-28176		
Vendor Reference:	RHSA-2023:1336		
Bugtraq ID:	-		
Service Modified:	10 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 23 Mar 2023 05:35:13 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 345

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Mozilla firefox is an open-source web browser, designed for standards compliance, performance, and portability...Security Fix(es): mozilla:

incorrect code generation during jit compilation (cve-2023-25751). Mozilla: memory safety bugs fixed in firefox 111 and firefox esr 102.9 (cve-2023-28176). Mozilla: potential out-of-bounds when accessing throttled streams (cve-2023-25752). Mozilla: invalid downcast in worklets (cve-2023-28162). Mozilla: url being dragged from a removed cross-origin iframe into the same tab triggered navigation (cve-2023-28164). 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-2023:1336 (https://access.redhat.com/errata/RHSA-2023:1336) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1336: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1336)

RESULTS:

Package	Installed Version	Required Version
firefox	102.6.0-1.el8_7.x86_64	102.9.0-3.el8_7

4 Red Hat Update for kernel (RHSA-2023:3349)

CVSS: 4.2 CVSS3.1: 7 Active

QID:	241571	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2023-32233		
Vendor Reference:	RHSA-2023:3349		
Bugtraq ID:	-		
Service Modified:	07 Jun 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 07 Jun 2023 10:56:07 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 104
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: netfilter: use-after-free in nf_tables when processing batch requests can lead to privilege escalation (cve-2023-32233). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux server - aus 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64. 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. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat codeready linux builder for x86_64 - extended update support 8.8 x86_64. Red hat codeready linux builder for power, little endian - extended update support 8.8 ppc64le. Red hat codeready linux builder for arm 64 - extended update support 8.8 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-2023:3349 (https://access.redhat.com/errata/RHSA-2023:3349) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3349: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3349)

RESULTS:

Package	Installed Version	Required Version
bpftool	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
kernel-core	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.13.1.el8_8
kernel-core	4.18.0-425.3.1.el8.x86_64	4.18.0-477.13.1.el8_8
kernel-core	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
kernel-tools	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
kernel-modules	4.18.0-425.3.1.el8.x86_64	4.18.0-477.13.1.el8_8
kernel-modules	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
kernel-modules	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.13.1.el8_8
kernel-tools-libs	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
kernel-headers	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
python3-perf	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8
kernel	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.13.1.el8_8
kernel	4.18.0-425.3.1.el8.x86_64	4.18.0-477.13.1.el8_8
kernel	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.13.1.el8_8

4 Red Hat Update for firefox (RHSA-2023:3590)

CVSS: 4 CVSS3.1: 8.5 Active

QID:	241723	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-34414, CVE-2023-34416		
Vendor Reference:	RHSA-2023:3590		
Bugtraq ID:	-		
Service Modified:	28 Jun 2023	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 16 Jun 2023 09:25:50 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 80

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Mozilla firefox is an open-source web browser, designed for standards compliance, performance, and portability...Security Fix(es): mozilla: click-jacking certificate exceptions through rendering lag (cve-2023-34414). Mozilla: memory safety bugs fixed in firefox 114 and firefox esr 102.12 (cve-2023-34416). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64..
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-2023:3590 (https://access.redhat.com/errata/RHSA-2023:3590) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3590: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3590)

RESULTS:

Package	Installed Version	Required Version
firefox	102.6.0-1.el8_7.x86_64	102.12.0-1.el8_8

4 Red Hat Update for firefox (RHSA-2023:3220) CVSS: 4 CVSS3.1: 7.7 Active

QID:	241547	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-32205, CVE-2023-32206, CVE-2023-32207, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215		
Vendor Reference:	RHSA-2023:3220		
Bugtraq ID:	-		
Service Modified:	10 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 23 May 2023 12:01:08 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 143
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Mozilla firefox is an open-source web browser, designed for standards compliance, performance, and portability...Security Fix(es): mozilla: browser prompts could have been obscured by popups (cve-2023-32205). Mozilla: crash in rlbox expat driver (cve-2023-32206). Mozilla: potential permissions request bypass via clickjacking (cve-2023-32207). Mozilla: memory safety bugs fixed in firefox 113 and firefox esr 102.11 (cve-2023-32215). Mozilla: content process crash due to invalid wasm code (cve-2023-32211). Mozilla: potential spoof due to obscured address bar (cve-2023-32212). Mozilla: potential memory corruption in filereader::doreaddata() (cve-2023-32213). <H2></H2> Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux server - aus 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3220 (https://access.redhat.com/errata/RHSA-2023:3220) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3220: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3220)

RESULTS:

Package	Installed Version	Required Version

firefox	102.6.0-1.el8_7.x86_64	102.11.0-2.el8_7

4 Red Hat Update for emacs (RHSA-2023:1930)

CVSS: 4 CVSS3.1: 6.8 Active

QID:	241375	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-28617		
Vendor Reference:	RHSA-2023:1930		
Bugtraq ID:	-		
Service Modified:	25 Apr 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 26 Apr 2023 10:27:43 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 231

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Gnu emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read e-mail and news...Security Fix(es): emacs: command injection vulnerability in org-mode (cve-2023-28617). <H2></H2> 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-2023:1930 (https://access.redhat.com/errata/RHSA-2023:1930) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1930: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1930)

RESULTS:

Package	Installed Version	Required Version
emacs-filesystem	26.1-7.el8.noarch	26.1-7.el8_7.1

4 Red Hat Update for python3 (RHSA-2023:0833)

CVSS: 4.2 CVSS3.1: 6.7 Active

QID:	241211	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2020-10735, CVE-2021-28861, CVE-2022-45061		
Vendor Reference:	RHSA-2023:0833		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems...Security Fix(es): python: int() type in pylong_fromstring() does not limit amount of digits converting text to int leading to dos (cve-2020-10735). Python: open redirection vulnerability in lib/http/server.py may lead to information disclosure (cve-2021-28861). Python: cpu denial of service via inefficient idna decoder (cve-2022-45061). 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-2023:0833 (https://access.redhat.com/errata/RHSA-2023:0833) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0833: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0833)

RESULTS:

Package	Installed Version	Required Version
python3-libs	3.6.8-48.el8_7.x86_64	3.6.8-48.el8_7.1
platform-python	3.6.8-48.el8_7.x86_64	3.6.8-48.el8_7.1

4 Red Hat Update for libwebp (RHSA-2023:2076)

CVSS: 4 CVSS3.1: 6.5 Active

QID:	241400	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-1999		
Vendor Reference:	RHSA-2023:2076		
Bugtraq ID:	-		
Service Modified:	06 Jul 2023	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.5
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 04 May 2023 04:14:33 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 206

Last Fixed: N/A

CVSS Environment:

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

THREAT:
The libwebp packages provide a library and tools for the webp graphics format. Webp is an image format with a lossy compression of digital photographic images. Webp consists of a codec based on the vp8 format, and a container based on the resource interchange file format (riff). Webmasters, web developers and browser developers can use webp to compress, archive, and distribute digital images more efficiently...Security Fix(es): mozilla: libwebp: double-free in libwebp (cve-2023-1999). 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-2023:2076 (https://access.redhat.com/errata/RHSA-2023:2076) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2076: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2076)

RESULTS:

Package	Installed Version	Required Version
libwebp	1.0.0-5.el8.x86_64	1.0.0-8.el8_7

4 Red Hat Update for emacs (RHSA-2023:3104)

CVSS: 4 CVSS3.1: 6.8 Active

QID:	241526	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-2491		
Vendor Reference:	RHSA-2023:3104		
Bugtraq ID:	-		
Service Modified:	26 May 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Gnu emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read e-mail and news...Security Fix(es): emacs: regression of cve-2023-28617 fixes in the Red Hat enterprise linux (cve-2023-2491). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux server - aus 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3104 (https://access.redhat.com/errata/RHSA-2023:3104) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3104: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3104)

RESULTS:

Package	Installed Version	Required Version
emacs-filesystem	26.1-7.el8.noarch	26.1-10.el8_8.2

4 Red Hat Update for webkit2gtk3 (RHSA-2023:2834) CVSS: 4.2 CVSS3.1: 7.9 Active

QID:	241497	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-32886, CVE-2022-32888, CVE-2022-32923, CVE-2022-42799, CVE-2022-42823, CVE-2022-42824, CVE-2022-42826, CVE-2022-42852, CVE-2022-42863, CVE-2022-42867, CVE-2022-46691, CVE-2022-46692, CVE-2022-46698, CVE-2022-46699, CVE-2022-46700, CVE-2023-23517, CVE-2023-23518, CVE-2023-25358, CVE-2023-25360, CVE-2023-25361, CVE-2023-25362, CVE-2023-25363		
Vendor Reference:	RHSA-2023:2834		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Red Hat has released a security update for webkit2gtk3 to fix the vulnerabilities.

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-2023:2834 (https://access.redhat.com/errata/RHSA-2023:2834) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2834: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2834)

RESULTS:

Package	Installed Version	Required Version
webkit2gtk3	2.36.7-1.el8_7.1.x86_64	2.38.5-1.el8
webkit2gtk3-jsc	2.36.7-1.el8_7.1.x86_64	2.38.5-1.el8

4 Red Hat Update for firefox (RHSA-2023:0288) CVSS: 4 CVSS3.1: 7.7 Active

QID:	241092	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0

Associated CVEs:	CVE-2022-46871, CVE-2022-46877, CVE-2023-23598, CVE-2023-23599, CVE-2023-23601, CVE-2023-23602, CVE-2023-23603, CVE-2023-23605		
Vendor Reference:	RHSA-2023:0288		
Bugtraq ID:	-		
Service Modified:	24 Jan 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Mozilla firefox is an open-source web browser, designed for standards compliance, performance, and portability...Security Fix(es): mozilla: libusrsctp library out of date (cve-2022-46871). Mozilla: arbitrary file read from gtk drag and drop on linux (cve-2023-23598). Mozilla: memory safety bugs fixed in firefox 109 and firefox esr 102.7 (cve-2023-23605). Mozilla: malicious command could be hidden in devtools output (cve-2023-23599). Mozilla: url being dragged from cross-origin iframe into same tab triggers navigation (cve-2023-23601). Mozilla: content security policy wasn't being correctly applied to websockets in webworkers (cve-2023-23602). Mozilla: fullscreen notification bypass (cve-2022-46877). Mozilla: calls to <code>console.log</code> allowed bypasing content security policy via format directive (cve-2023-23603). 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-2023:0288 (https://access.redhat.com/errata/RHSA-2023:0288) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0288: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0288)

RESULTS:

Package	Installed Version	Required Version
firefox	102.6.0-1.el8_7.x86_64	102.7.0-1.el8_7

4 Red Hat Update for webkit2gtk3 (RHSA-2023:3433) CVSS: 4.5 CVSS3.1: 8.2 Active

QID:	241577	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.5
Associated CVEs:	CVE-2023-28204, CVE-2023-32373		
Vendor Reference:	RHSA-2023:3433		
Bugtraq ID:	-		
Service Modified:	28 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	8.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 07 Jun 2023 10:56:07 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 104

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Webkitgtk is the port of the portable web rendering engine webkit to the gtk platform...Security Fix(es): webkitgtk: a use-after-free when processing maliciously crafted web content (cve-2023-32373). Webkitgtk: an out-of-bounds read when processing malicious content (cve-2023-28204). <H2></H2> Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux server - aus 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3433 (https://access.redhat.com/errata/RHSA-2023:3433) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3433: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3433)

RESULTS:

Package	Installed Version	Required Version
webkit2gtk3	2.36.7-1.el8_7.1.x86_64	2.38.5-1.el8_8.4
webkit2gtk3-jsc	2.36.7-1.el8_7.1.x86_64	2.38.5-1.el8_8.4

4 Red Hat Update for nss (RHSA-2023:1252)

CVSS: 4 CVSS3.1: 7.7 Active

QID:	241262	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-0767		
Vendor Reference:	RHSA-2023:1252		
Bugtraq ID:	-		
Service Modified:	10 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 23 Mar 2023 05:35:13 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 345

Last Fixed: N/A

CVSS Environment:

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

THREAT:
Network security services (nss) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications...Security Fix(es): nss: arbitrary memory write via pkcs 12 (cve-2023-0767). <H2></H2> 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-2023:1252 (https://access.redhat.com/errata/RHSA-2023:1252) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1252: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1252)

RESULTS:

Package	Installed Version	Required Version
nss	3.79.0-10.el8_6.x86_64	3.79.0-11.el8_7
nss-sysinit	3.79.0-10.el8_6.x86_64	3.79.0-11.el8_7
nss-softokn	3.79.0-10.el8_6.x86_64	3.79.0-11.el8_7
nss-util	3.79.0-10.el8_6.x86_64	3.79.0-11.el8_7
nss-softokn-freebl	3.79.0-10.el8_6.x86_64	3.79.0-11.el8_7

4 Red Hat Update for kernel security (RHSA-2023:2951)

CVSS: 5.6 CVSS3.1: 7.9 Active

QID:	241504	CVSS Base:	7.2
Category:	RedHat	CVSS Temporal:	5.6
Associated CVEs:	CVE-2021-26341, CVE-2021-33655, CVE-2021-33656, CVE-2022-1462, CVE-2022-1679, CVE-2022-1789, CVE-2022-2196, CVE-2022-2663, CVE-2022-3028, CVE-2022-3239, CVE-2022-3522, CVE-2022-3524, CVE-2022-3564, CVE-2022-3566, CVE-2022-3567, CVE-2022-3619, CVE-2022-3623, CVE-2022-3625, CVE-2022-3628, CVE-2022-3707, CVE-2022-4129, CVE-2022-20141, CVE-2022-25265, CVE-2022-30594, CVE-2022-39188, CVE-2022-39189, CVE-2022-41218, CVE-2022-41674, CVE-2022-42703, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722, CVE-2022-43750, CVE-2022-47929, CVE-2023-0394, CVE-2023-0461, CVE-2023-1195, CVE-2023-1582, CVE-2023-23454		
Vendor Reference:	RHSA-2023:2951		
Bugtraq ID:	-		
Service Modified:	05 Jul 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Red Hat has released a security update for kernel security to fix the vulnerabilities.

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-2023:2951 (https://access.redhat.com/errata/RHSA-2023:2951) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2951: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2951)

RESULTS:

Package	Installed Version	Required Version
kernel-core	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.10.1.el8_8
kernel-core	4.18.0-425.3.1.el8.x86_64	4.18.0-477.10.1.el8_8
kernel-core	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
kernel-headers	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
kernel-tools	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
kernel-tools-libs	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
bpftool	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
kernel-modules	4.18.0-425.3.1.el8.x86_64	4.18.0-477.10.1.el8_8
kernel-modules	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
kernel-modules	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.10.1.el8_8
python3-perf	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8
kernel	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.10.1.el8_8
kernel	4.18.0-425.3.1.el8.x86_64	4.18.0-477.10.1.el8_8
kernel	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.10.1.el8_8

4 Red Hat Update for webkit2gtk3 (RHSA-2023:0902)

CVSS: 4.5 CVSS3.1: 8.2 Active

QID:	241212	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.5
Associated CVEs:	CVE-2023-23529		
Vendor Reference:	RHSA-2023:0902		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	8.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 373
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Webkitgtk is the port of the portable web rendering engine webkit to the gtk.platform...Security Fix(es): webkitgtk: processing maliciously crafted web content may be exploited for arbitrary code execution (cve-2023-23529). 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-2023:0902 (https://access.redhat.com/errata/RHSA-2023:0902) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0902: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0902)

RESULTS:

Package	Installed Version	Required Version
webkit2gtk3-jsc	2.36.7-1.el8_7.1.x86_64	2.36.7-1.el8_7.2
webkit2gtk3	2.36.7-1.el8_7.1.x86_64	2.36.7-1.el8_7.2

4 Red Hat Update for libksba (RHSA-2023:0625)

CVSS: 4 CVSS3.1: 8.5 Active

QID:	241168	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-47629		
Vendor Reference:	RHSA-2023:0625		
Bugtraq ID:	-		
Service Modified:	05 May 2023	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:	Open		

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

Last Fixed: N/A

CVSS Environment:

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

THREAT:
Ksba (pronounced kasbah) is a library to make x.509 certificates as well as the cms easily accessible by other applications. Both specifications are building blocks of s/mime and tls...Security Fix(es): libksba: integer overflow to code executiona (cve-2022-47629). 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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:0625 (https://access.redhat.com/errata/RHSA-2023:0625) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0625: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0625)

RESULTS:

Package	Installed Version	Required Version
libksba	1.3.5-8.el8_6.x86_64	1.3.5-9.el8_7

4 Red Hat Update for firefox (RHSA-2023:1787)

CVSS: 4 CVSS3.1: 7.7 Active

QID:	241345	CVSS Base:	5.4 [1]

Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-1945, CVE-2023-29533, CVE-2023-29535, CVE-2023-29536, CVE-2023-29539, CVE-2023-29541, CVE-2023-29548, CVE-2023-29550		
Vendor Reference:	RHSA-2023:1787		
Bugtraq ID:	-		
Service Modified:	10 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 20 Apr 2023 09:53:21 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 251

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Mozilla firefox is an open-source web browser, designed for standards compliance, performance, and portability...Security Fix(es): mfsa-tmp-2023-0001 mozilla: double-free in libwebp (bz#2186102). Mozilla: fullscreen notification obscured (cve-2023-29533). Mozilla: potential memory corruption following garbage collector compaction (cve-2023-29535). Mozilla: invalid free from javascript code (cve-2023-29536). Mozilla: memory safety bugs fixed in firefox 112 and firefox esr 102.10 (cve-2023-29550). Mozilla: memory corruption in safe browsing code (cve-2023-1945). Mozilla: content-disposition filename truncation leads to reflected file download (cve-2023-29539). Mozilla: files with malicious extensions could have been downloaded unsafely on linux (cve-2023-29541). Mozilla: incorrect optimization result on arm64 (cve-2023-29548). 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-2023:1787 (https://access.redhat.com/errata/RHSA-2023:1787) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1787: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1787)

RESULTS:

Package	Installed Version	Required Version
firefox	102.6.0-1.el8_7.x86_64	102.10.0-1.el8_7

4 Red Hat Update for kernel (RHSA-2023:0832)

CVSS: 4.2 CVSS3.1: 6.7 Active

QID:	241209	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-2873, CVE-2022-41222, CVE-2022-43945		
Vendor Reference:	RHSA-2023:0832		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

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: mm/mremap.c use-after-free vulnerability (cve-2022-41222). Kernel: nfsd buffer overflow by rpc message over tcp with garbage data (cve-2022-43945). Kernel: an out-of-bounds vulnerability in i2c-ismt driver (cve-2022-2873). 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-2023:0832 (https://access.redhat.com/errata/RHSA-2023:0832) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0832: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0832)

RESULTS:

Package	Installed Version	Required Version
bpftool	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
python3-perf	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
kernel-headers	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
kernel-tools-libs	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
kernel	4.18.0-372.32.1.el8_6.x86_64	4.18.0-425.13.1.el8_7
kernel	4.18.0-425.3.1.el8.x86_64	4.18.0-425.13.1.el8_7
kernel	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
kernel-tools	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
kernel-modules	4.18.0-425.3.1.el8.x86_64	4.18.0-425.13.1.el8_7
kernel-modules	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7
kernel-modules	4.18.0-372.32.1.el8_6.x86_64	4.18.0-425.13.1.el8_7
kernel-core	4.18.0-372.32.1.el8_6.x86_64	4.18.0-425.13.1.el8_7
kernel-core	4.18.0-425.3.1.el8.x86_64	4.18.0-425.13.1.el8_7
kernel-core	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.13.1.el8_7

4 Red Hat Update for curl (RHSA-2023:1140)

CVSS: 4.2 CVSS3.1: 5.9 Active

QID:	241245	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2023-23916		
Vendor Reference:	RHSA-2023:1140		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	6.5
User Modified:	-	CVSS3.1 Temporal:	5.9
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

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: http multi-header compression denial of service (cve-2023-23916). 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-2023:1140 (https://access.redhat.com/errata/RHSA-2023:1140) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1140: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1140)

RESULTS:

Package	Installed Version	Required Version
libcurl	7.61.1-25.el8_7.1.x86_64	7.61.1-25.el8_7.3
curl	7.61.1-25.el8_7.1.x86_64	7.61.1-25.el8_7.3
libcurl-devel	7.61.1-25.el8_7.1.x86_64	7.61.1-25.el8_7.3

4 Red Hat Update for kernel security (RHSA-2023:1566)

CVSS: 4.5 CVSS3.1: 7.2 Active

QID:	241324	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.5
Associated CVEs:	CVE-2022-4269, CVE-2022-4378, CVE-2023-0266, CVE-2023-0386		
Vendor Reference:	RHSA-2023:1566		
Bugtraq ID:	-		
Service Modified:	01 Jul 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06 Apr 2023 05:37:18 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 298

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: stack overflow in do_proc_dointvec and proc_skip_spaces (cve-2022-4378). Alsa: pcm: move rwsem lock inside snd_ctl_elem_read to prevent uaf (cve-2023-0266). Kernel: fuse filesystem low-privileged user privileges escalation (cve-2023-0386). Kernel: net: cpu soft lockup in tc mirred egress-to-ingress action (cve-2022-4269). 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-2023:1566 (https://access.redhat.com/errata/RHSA-2023:1566) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1566: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1566)

RESULTS:

Package	Installed Version	Required Version
kernel-tools-libs	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
kernel-core	4.18.0-372.32.1.el8_6.x86_64	4.18.0-425.19.2.el8_7
kernel-core	4.18.0-425.3.1.el8.x86_64	4.18.0-425.19.2.el8_7
kernel-core	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
kernel-modules	4.18.0-425.3.1.el8.x86_64	4.18.0-425.19.2.el8_7
kernel-modules	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
kernel-modules	4.18.0-372.32.1.el8_6.x86_64	4.18.0-425.19.2.el8_7
python3-perf	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
bpftool	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
kernel-headers	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
kernel-tools	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7
kernel	4.18.0-372.32.1.el8_6.x86_64	4.18.0-425.19.2.el8_7
kernel	4.18.0-425.3.1.el8.x86_64	4.18.0-425.19.2.el8_7
kernel	4.18.0-425.10.1.el8_7.x86_64	4.18.0-425.19.2.el8_7

4 Red Hat Update for samba (RHSA-2023:0838)

CVSS: 4 CVSS3.1: 7.1 Active

QID:	241203	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-38023		
Vendor Reference:	RHSA-2023:0838		
Bugtraq ID:	-		
Service Modified:	22 Feb 2023	CVSS3.1 Base:	8.1
User Modified:	-	CVSS3.1 Temporal:	7.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 373
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Samba is an open-source implementation of the server message block (smb) protocol and the related common internet file system (cifs) protocol, which allow pc-compatible machines to share files, printers, and various information...Security Fix(es): samba: rc4/hmac-md5 netlogon secure channel is weak and should be avoided (cve-2022-38023). 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. Red hat codeready linux builder for ibm z systems 8 s390x..
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-2023:0838 (https://access.redhat.com/errata/RHSA-2023:0838) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0838: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0838)

RESULTS:

Package	Installed Version	Required Version
samba-common	4.16.4-2.el8.noarch	4.16.4-4.el8_7
samba-client-libs	4.16.4-2.el8.x86_64	4.16.4-4.el8_7
samba-common-libs	4.16.4-2.el8.x86_64	4.16.4-4.el8_7
libwbclient	4.16.4-2.el8.x86_64	4.16.4-4.el8_7
libsmbclient	4.16.4-2.el8.x86_64	4.16.4-4.el8_7

3 Red Hat Update for device-mapper-multipath (RHSA-2023:2948) CVSS: 4.2 CVSS3.1: 7 Active

QID:	241530	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-41973		
Vendor Reference:	RHSA-2023:2948		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
The device-mapper-multipath packages provide tools that use the device-mapper multipath kernel module to manage multipath devices...Security Fix(es): device-mapper-multipath: multipathd: insecure handling of files in /dev/shm leading to symlink attack (cve-2022-41973).
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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:2948 (https://access.redhat.com/errata/RHSA-2023:2948) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2948: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2948)

RESULTS:

Package	Installed Version	Required Version
device-mapper-multipath	0.8.4-28.el8_7.1.x86_64	0.8.4-37.el8
kpartx	0.8.4-28.el8_7.1.x86_64	0.8.4-37.el8
device-mapper-multipath-libs	0.8.4-28.el8_7.1.x86_64	0.8.4-37.el8

3 Red Hat Update for emacs (RHSA-2023:3042) CVSS: 4 CVSS3.1: 6.8 Active

QID:	241509	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-45939		
Vendor Reference:	RHSA-2023:3042		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Gnu emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read e-mail and news...Security Fix(es): emacs: ctags local command execution vulnerability (cve-2022-45939). 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-2023:3042 (https://access.redhat.com/errata/RHSA-2023:3042) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3042: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3042)

RESULTS:

Package	Installed Version	Required Version
emacs-filesystem	26.1-7.el8.noarch	26.1-9.el8

3 Red Hat Update for libssh (RHSA-2023:3839) CVSS: 4.2 CVSS3.1: 5.9 Active

QID:	241759	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2023-1667, CVE-2023-2283		
Vendor Reference:	RHSA-2023:3839		
Bugtraq ID:	-		
Service Modified:	28 Jun 2023	CVSS3.1 Base:	6.5
User Modified:	-	CVSS3.1 Temporal:	5.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 29 Jun 2023 07:27:31 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 47

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Libssh is a library which implements the ssh protocol. It can be used to implement client and server applications...Security Fix(es): libssh: null pointer dereference during rekeying with algorithm guessing (cve-2023-1667). Libssh: authorization bypass in pki_verify_data_signature (cve-2023-2283). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3839 (https://access.redhat.com/errata/RHSA-2023:3839) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3839: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3839)

RESULTS:

Package	Installed Version	Required Version
libssh-config	0.9.6-3.el8.noarch	0.9.6-10.el8_8
libssh	0.9.6-3.el8.x86_64	0.9.6-10.el8_8

3 Red Hat Update for python-setuptools (RHSA-2023:0835) CVSS: 4.2 CVSS3.1: 5.3 Active

QID:	241207	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-40897		
Vendor Reference:	RHSA-2023:0835		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	5.9
User Modified:	-	CVSS3.1 Temporal:	5.3
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The python-setuptools package provides a collection of enhancements to python distribution utilities allowing convenient building and distribution of python packages...Security Fix(es): pypa-setuptools: regular expression denial of service (redos) in package_index.py (cve-2022-40897). 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-2023:0835 (https://access.redhat.com/errata/RHSA-2023:0835) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0835: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0835)

RESULTS:

Package	Installed Version	Required Version
python3-setuptools	39.2.0-6.el8.noarch	39.2.0-6.el8_7.1
platform-python-setuptools	39.2.0-6.el8.noarch	39.2.0-6.el8_7.1
python3-setuptools-wheel	39.2.0-6.el8.noarch	39.2.0-6.el8_7.1

3 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2023:2757) CVSS: 3.6 CVSS3.1: 7 Active

QID:	241506	CVSS Base:	4.6
Category:	RedHat	CVSS Temporal:	3.6
Associated CVEs:	CVE-2021-46790, CVE-2022-3165, CVE-2022-30784, CVE-2022-30786, CVE-2022-30788, CVE-2022-30789, CVE-2023-1018		
Vendor Reference:	RHSA-2023:2757		
Bugtraq ID:	-		
Service Modified:	01 Jun 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

Integrity Requirement: -
Availability Requirement: -

THREAT:
Kernel-based virtual machine (kvm) offers a full virtualization solution for linux on numerous hardware platforms. The virt:rhel module contains packages which provide user-space components used to run virtual machines using kvm. The packages also provide apis for managing and
interacting with the virtualized systems...Security Fix(es): ntfs-3g: heap-based buffer overflow in ntfsck (cve-2021-46790). Qemu: vnc: integer underflow in vnc_client_cut_text_ext leads to cpu exhaustion (cve-2022-3165). Ntfs-3g: crafted ntfs image can cause heap exhaustion in ntfs_get_attribute_value (cve-2022-30784). Ntfs-3g: crafted ntfs image can cause a heap-based buffer overflow in ntfs_names_full_collate (cve-2022-30786). Ntfs-3g: crafted ntfs image can cause a heap-based buffer overflow in ntfs_mft_rec_alloc (cve-2022-30788). Ntfs-3g: crafted ntfs image can cause a heap-based buffer overflow in ntfs_check_log_client_array (cve-2022-30789). Tpm2: tcg tpm2.0 implementations vulnerable to memory corruption (cve-2023-1018). <H2></H2> 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. Red hat codeready linux builder for ibm z systems 8 s390x..
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-2023:2757 (https://access.redhat.com/errata/RHSA-2023:2757) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2757: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2757)

RESULTS:

Package	Installed Version	Required Version
libtpms	0.9.1-1.20211126git1ff6fe1f43.module+ el8.7.0+16689+53d59bc2.x86_64	0.9.1-2.20211126git1ff6fe1f43.module +el8.8.0+18453+e0bf0d1d
swtpm-libs	0.7.0-4.20211109gitb79fd91.module+el8 .7.0+16689+53d59bc2.x86_64	0.7.0-4.20211109gitb79fd91.module+el 8.8.0+16781+9f4724c2
swtpm-tools	0.7.0-4.20211109gitb79fd91.module+el8 .7.0+16689+53d59bc2.x86_64	0.7.0-4.20211109gitb79fd91.module+el 8.8.0+16781+9f4724c2
swtpm	0.7.0-4.20211109gitb79fd91.module+el8 .7.0+16689+53d59bc2.x86_64	0.7.0-4.20211109gitb79fd91.module+el 8.8.0+16781+9f4724c2
sgabios-bin	0.20170427git-3.module+el8.7.0+16689+ 53d59bc2.noarch	0.20170427git-3.module+el8.8.0+16781+9f4724c2
libvirt-daemon-driver-qemu	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-logical	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-disk	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-mpath	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-kvm	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-rbd	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-libs	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-secret	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-network	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-iscsi-direct	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-interface	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-core	8.0.0-10.1.module+el8.7.0+17192+cbc24 49b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d

libvirt-daemon-driver-storage-gluster	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-scsi	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-config-network	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-nwfilter	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-nodedev	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libvirt-daemon-driver-storage-iscsi	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.module+el8.8.0+18453+e0bf0d1d
libiscsi	1.18.0-8.module+el8.7.0+16689+53d59bc2.x86_64	1.18.0-8.module+el8.8.0+16781+9f4724c2
seabios-bin	1.16.0-3.module+el8.7.0+16689+53d59bc2.noarch	1.16.0-3.module+el8.8.0+16781+9f4724c2
seavgabios-bin	1.16.0-3.module+el8.7.0+16689+53d59bc2.noarch	1.16.0-3.module+el8.8.0+16781+9f4724c2
netcf-libs	0.2.8-12.module+el8.7.0+16689+53d59bc2.x86_64	0.2.8-12.module+el8.8.0+16781+9f4724c2
qemu-kvm-block-curl	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-gluster	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-hw-usbredir	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-common	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-core	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-docs	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-rbd	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-iscsi	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-ui-opengl	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-ui-spice	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-ssh	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-guest-agent	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-img	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e

3 Red Hat Update for net-snmp (RHSA-2023:2969)

CVSS: 4.2 CVSS3.1: 5.9 Active

QID:	241494	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-44792, CVE-2022-44793		
Vendor Reference:	RHSA-2023:2969		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	6.5
User Modified:	-	CVSS3.1 Temporal:	5.9
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The net-snmp packages provide various libraries and tools for the simple network management protocol (snmp), including an snmp library, an

extensible agent, tools for requesting or setting information from snmp agents, tools for generating and handling snmp traps, a version of the netstat command which uses snmp, and a tk/perl management information base (mib) browser...Security Fix(es): net-snmp: null pointer exception when handling ipdefaulttl (cve-2022-44792). Net-snmp: null pointer exception when handling pv6ipforwarding (cve-2022-44793). <H2></H2> 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-2023:2969 (https://access.redhat.com/errata/RHSA-2023:2969) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2969: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2969)

RESULTS:

Package	Installed Version	Required Version
net-snmp-agent-libs	5.8-25.el8_7.1.x86_64	5.8-27.el8
net-snmp-utils	5.8-25.el8_7.1.x86_64	5.8-27.el8
net-snmp	5.8-25.el8_7.1.x86_64	5.8-27.el8
net-snmp-libs	5.8-25.el8_7.1.x86_64	5.8-27.el8

3 Red Hat Update for unbound (RHSA-2023:2771) CVSS: 4 CVSS3.1: 6.5 Active

QID:	241518	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-3204		
Vendor Reference:	RHSA-2023:2771		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.5
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
The unbound packages provide a validating, recursive, and caching dns or dnssec resolver. .. Security fix(es): unbound: nrdelegation attack leads to uncontrolled resource consumption (non-responsive delegation attack) (cve-2022-3204). 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-2023:2771 (https://access.redhat.com/errata/RHSA-2023:2771) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

RHSA-2023:2771: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2771)

RESULTS:

Package	Installed Version	Required Version
python3-unbound	1.16.2-2.el8.x86_64	1.16.2-5.el8
unbound-libs	1.16.2-2.el8.x86_64	1.16.2-5.el8

3 Red Hat Update for systemd (RHSA-2023:0837) CVSS: 4.2 CVSS3.1: 5 Active

QID:	241208	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-4415		
Vendor Reference:	RHSA-2023:0837		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:23:42 PM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 373

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The systemd packages contain systemd, a system and service manager for linux, compatible with the sysv and lsb init scripts. It provides aggressive parallelism capabilities, uses socket and d-bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount points, and implements an elaborate transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit...Security Fix(es): systemd: local information leak due to systemd-coredump not respecting fs.suid_dumpable kernel setting (cve-2022-4415). 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-2023:0837 (https://access.redhat.com/errata/RHSA-2023:0837) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:0837: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:0837)

RESULTS:

Package	Installed Version	Required Version
systemd-libs	239-68.el8_7.2.x86_64	239-68.el8_7.4
systemd-udev	239-68.el8_7.2.x86_64	239-68.el8_7.4
systemd-pam	239-68.el8_7.2.x86_64	239-68.el8_7.4
systemd	239-68.el8_7.2.x86_64	239-68.el8_7.4
systemd-container	239-68.el8_7.2.x86_64	239-68.el8_7.4

3 Red Hat Update for libtiff (RHSA-2023:2883) CVSS: 4.2 CVSS3.1: 7.9 Active

QID:	241478	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-3627, CVE-2022-3970		
Vendor Reference:	RHSA-2023:2883		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The libtiff packages contain a library of functions for manipulating tagged image file format (tiff) files...Security Fix(es): libtiff: out-of-bounds write in _tiffmemcpy in libtiff/tif_unix.c (cve-2022-3627). Libtiff: integer overflow in function tiffreadrgbatileext of the file (cve-2022-3970). 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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:2883 (https://access.redhat.com/errata/RHSA-2023:2883) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2883: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2883)

RESULTS:

Package	Installed Version	Required Version
libtiff	4.0.9-26.el8_7.x86_64	4.0.9-27.el8

3 Red Hat Update for poppler (RHSA-2023:2810) CVSS: 4.2 CVSS3.1: 7 Active

QID:	241484	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-38784		
Vendor Reference:	RHSA-2023:2810		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Poppler is a portable document format (pdf) rendering library, used by applications such as evince...Security Fix(es): poppler: integer overflow in jbig2 decoder using malformed files (cve-2022-38784). <H2></H2> 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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:2810 (https://access.redhat.com/errata/RHSA-2023:2810) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2810: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2810)

RESULTS:

Package	Installed Version	Required Version
poppler-glib	20.11.0-5.el8.x86_64	20.11.0-6.el8
poppler	20.11.0-5.el8.x86_64	20.11.0-6.el8

3 Red Hat Update for bind (RHSA-2023:3002) CVSS: 4 CVSS3.1: 4.6 Active

QID:	241498	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-2795		
Vendor Reference:	RHSA-2023:3002		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	5.3
User Modified:	-	CVSS3.1 Temporal:	4.6
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The berkeley internet name domain (bind) is an implementation of the domain name system (dns) protocols. Bind includes a dns server (named); a resolver library (routines for applications to use when interfacing with dns); and tools for verifying that the dns server is operating correctly...Security Fix(es): bind: processing large delegations may severely degrade resolver performance (cve-2022-2795). <H2></H2> 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-2023:3002 (https://access.redhat.com/errata/RHSA-2023:3002) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3002: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3002)

RESULTS:

Package	Installed Version	Required Version
bind-license	9.11.36-5.el8_7.2.noarch	9.11.36-8.el8
bind-export-libs	9.11.36-5.el8_7.2.x86_64	9.11.36-8.el8
bind-libs	9.11.36-5.el8_7.2.x86_64	9.11.36-8.el8
python3-bind	9.11.36-5.el8_7.2.noarch	9.11.36-8.el8
bind-utils	9.11.36-5.el8_7.2.x86_64	9.11.36-8.el8
bind-libs-lite	9.11.36-5.el8_7.2.x86_64	9.11.36-8.el8

3 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2023:3822)

CVSS: 4 CVSS3.1: 4.8 Active

QID:	241756	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-2700		
Vendor Reference:	RHSA-2023:3822		
Bugtraq ID:	-		
Service Modified:	28 Jun 2023	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	4.8
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 29 Jun 2023 07:27:31 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 47
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Red Hat has released a security update for virt:rhel and virt-devel:rhel to fix the vulnerabilities.

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-2023:3822 (https://access.redhat.com/errata/RHSA-2023:3822) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3822: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3822)

RESULTS:

Package	Installed Version	Required Version
libtpms	0.9.1-1.20211126git1ff6fe1f43.module+el8.7.0+16689+53d59bc2.x86_64	0.9.1-2.20211126git1ff6fe1f43.module+el8.8.0+18453+1482ba89
swtpm-libs	0.7.0-4.20211109gitb79fd91.module+el8.7.0+16689+53d59bc2.x86_64	0.7.0-4.20211109gitb79fd91.module+el8.8.0+16781+9f4724c2
swtpm-tools	0.7.0-4.20211109gitb79fd91.module+el8.7.0+16689+53d59bc2.x86_64	0.7.0-4.20211109gitb79fd91.module+el8.8.0+16781+9f4724c2
swtpm	0.7.0-4.20211109gitb79fd91.module+el8.7.0+16689+53d59bc2.x86_64	0.7.0-4.20211109gitb79fd91.module+el8.8.0+16781+9f4724c2
sgabios-bin	0.20170427git-3.module+el8.7.0+16689+53d59bc2.noarch	0.20170427git-3.module+el8.8.0+16781+9f4724c2
libvirt-daemon-driver-storage-iscsi	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-kvm	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-mpath	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-nwfilter	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-core	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-logical	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-interface	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-config-network	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-rbd	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-nodedev	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-disk	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-secret	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-libs	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-qemu	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-gluster	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-network	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-scsi	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage-iscsi-direct	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
libvirt-daemon-driver-storage	8.0.0-10.1.module+el8.7.0+17192+cbc2449b.x86_64	8.0.0-19.2.module+el8.8.0+18944+7f5acf75
seabios-bin	1.16.0-3.module+el8.7.0+16689+53d59bc2.noarch	1.16.0-3.module+el8.8.0+16781+9f4724c2
seavgabios-bin	1.16.0-3.module+el8.7.0+16689+53d59bc2.noarch	1.16.0-3.module+el8.8.0+16781+9f4724c2
qemu-kvm	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-guest-agent	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-iscsi	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-common	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-hw-usbredir	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-ssh	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-ui-opengl	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-docs	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-core	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e

qemu-kvm-block-rbd	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-ui-spice	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-curl	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-img	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
qemu-kvm-block-gluster	6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	6.2.0-32.module+el8.8.0+18361+9f407f6e
libiscsi	1.18.0-8.module+el8.7.0+16689+53d59bc2.x86_64	1.18.0-8.module+el8.8.0+16781+9f4724c2
netcf-libs	0.2.8-12.module+el8.7.0+16689+53d59bc2.x86_64	0.2.8-12.module+el8.8.0+16781+9f4724c2

3 Red Hat Update for freerdp (RHSA-2023:2851) CVSS: 4 CVSS3.1: 6.5 Active

QID:	241541	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-39282, CVE-2022-39283, CVE-2022-39316, CVE-2022-39317, CVE-2022-39318, CVE-2022-39319, CVE-2022-39320, CVE-2022-39347, CVE-2022-41877		
Vendor Reference:	RHSA-2023:2851		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Freerdp is a free implementation of the remote desktop protocol (rdp), released under the apache license. The xfreerdp client can connect to rdp servers such as microsoft windows machines, xrdp, and virtualbox...Security Fix(es): freerdp: clients using `/parallel` command line switch might read uninitialized data (cve-2022-39282). Freerdp: clients using the `/video` command line switch might read uninitialized data (cve-2022-39283). Freerdp: out of bounds read in zgfx decoder (cve-2022-39316). Freerdp: undefined behaviour in zgfx decoder (cve-2022-39317). Freerdp: division by zero in urbdrc channel (cve-2022-39318). Freerdp: missing length validation in urbdrc channel (cve-2022-39319). Freerdp: heap buffer overflow in urbdrc channel (cve-2022-39320). Freerdp: missing path sanitation with `drive` channel (cve-2022-39347). Freerdp: missing input length validation in `drive` channel (cve-2022-41877). 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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:2851 (https://access.redhat.com/errata/RHSA-2023:2851) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2851: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2851)

RESULTS:

Package	Installed Version	Required Version
freerdp-libs	2.2.0-8.el8.x86_64	2.2.0-10.el8
libwinpr	2.2.0-8.el8.x86_64	2.2.0-10.el8

3 Red Hat Update for sqlite (RHSA-2023:3840) CVSS: 4.2 CVSS3.1: 5 Active

QID:	241758	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2020-24736		
Vendor Reference:	RHSA-2023:3840		
Bugtraq ID:	-		
Service Modified:	29 Jun 2023	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.0
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 29 Jun 2023 07:27:31 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 47

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Sqlite is a c library that implements an sql database engine. A large subset of sql92 is supported. A complete database is stored in a single disk file. The api is designed for convenience and ease of use. Applications that link against sqlite can enjoy the power and flexibility of an sql database without the administrative hassles of supporting a separate database server...Security Fix(es): sqlite: crash due to misuse of window functions. (Cve-2020-24736). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3840 (https://access.redhat.com/errata/RHSA-2023:3840) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3840: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3840)

RESULTS:

Package	Installed Version	Required Version
sqlite	3.26.0-17.el8_7.x86_64	3.26.0-18.el8_8
sqlite-libs	3.26.0-17.el8_7.x86_64	3.26.0-18.el8_8
sqlite-devel	3.26.0-17.el8_7.x86_64	3.26.0-18.el8_8

3 Red Hat Update for xorg-x11-server (RHSA-2023:2806) CVSS: 4 CVSS3.1: 7.7 Active

QID:	241510	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-3550, CVE-2022-3551, CVE-2022-4283, CVE-2022-46340, CVE-2022-46341, CVE-2022-46342, CVE-2022-46343, CVE-2022-46344, CVE-2023-0494		
Vendor Reference:	RHSA-2023:2806		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7

Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
X.org is an open-source implementation of the x window system. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon...Security Fix(es): xorg-x11-server: buffer overflow in _getcountedstring() in xkb/xkb.c (cve-2022-3550). Xorg-x11-server: xkbgetkbdbyname use-after-free (cve-2022-4283). Xorg-x11-server: xtestswapfakeinput stack overflow (cve-2022-46340). Xorg-x11-server: xipassiveungrab out-of-bounds access (cve-2022-46341). Xorg-x11-server: xvdiselectvideonotify use-after-free (cve-2022-46342). Xorg-x11-server: screensaversetattributes use-after-free (cve-2022-46343). Xorg-x11-server: xichangeproperty out-of-bounds access (cve-2022-46344). Xorg-x11-server: deepcopypointerclasses use-after-free leads to privilege elevation (cve-2023-0494). Xorg-x11-server: memory leak in procxkbgetkbdbyname() in xkb/xkb.c (cve-2022-3551). 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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:2806 (https://access.redhat.com/errata/RHSA-2023:2806) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2806: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2806)

RESULTS:

Package	Installed Version	Required Version
xorg-x11-server-common	1.20.11-9.el8.x86_64	1.20.11-15.el8
xorg-x11-server-Xorg	1.20.11-9.el8.x86_64	1.20.11-15.el8

3 Red Hat Update for libtiff (RHSA-2023:3827) CVSS: 4.2 CVSS3.1: 5 Active

QID:	241755	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-48281		
Vendor Reference:	RHSA-2023:3827		
Bugtraq ID:	-		
Service Modified:	29 Jun 2023	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.0
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 29 Jun 2023 07:27:31 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 47
Last Fixed: N/A

CVSS Environment:

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

THREAT:

The libtiff packages contain a library of functions for manipulating tagged image file format (tiff) files...Security Fix(es): libtiff: heap-based buffer overflow in processcropselections() in tools/tiffcrop.c (cve-2022-48281). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64. Red hat codeready linux builder for x86_64 8 x86_64. Red hat codeready linux builder for arm 64 8 aarch64. Red hat codeready linux builder for ibm z systems 8 s390x. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat codeready linux builder for power, little endian 8 ppc64le. Red hat codeready linux builder for x86_64 - extended update support 8.8 x86_64. Red hat codeready linux builder for power, little endian - extended update support 8.8 ppc64le. Red hat codeready linux builder for ibm z systems - extended update support 8.8 s390x. Red hat codeready linux builder for arm 64 - extended update support 8.8 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-2023:3827 (https://access.redhat.com/errata/RHSA-2023:3827) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3827: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3827)

RESULTS:

Package	Installed Version	Required Version
libtiff	4.0.9-26.el8_7.x86_64	4.0.9-28.el8_8

3 Red Hat Update for curl (RHSA-2023:3106)

CVSS: 4.2 CVSS3.1: 5.3 Active

QID:	241501	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2023-27535		
Vendor Reference:	RHSA-2023:3106		
Bugtraq ID:	-		
Service Modified:	30 Jun 2023	CVSS3.1 Base:	5.9
User Modified:	-	CVSS3.1 Temporal:	5.3
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

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: ftp too eager connection reuse (cve-2023-27535). 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-2023:3106 (https://access.redhat.com/errata/RHSA-2023:3106) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3106: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3106)

RESULTS:

Package	Installed Version	Required Version
curl	7.61.1-25.el8_7.1.x86_64	7.61.1-30.el8_8.2
libcurl	7.61.1-25.el8_7.1.x86_64	7.61.1-30.el8_8.2
libcurl-devel	7.61.1-25.el8_7.1.x86_64	7.61.1-30.el8_8.2

3 Red Hat Update for kernel security (RHSA-2023:3847)

CVSS: 4 CVSS3.1: 6.1 Active

QID:	241752	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-28466		
Vendor Reference:	RHSA-2023:3847		
Bugtraq ID:	-		
Service Modified:	28 Jun 2023	CVSS3.1 Base:	7.0
User Modified:	-	CVSS3.1 Temporal:	6.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 29 Jun 2023 07:27:31 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 47
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: tls: race condition in do_tls_getsockopt may lead to use-after-free or null pointer dereference (cve-2023-28466). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64. 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. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat codeready linux builder for x86_64 - extended update support 8.8 x86_64. Red hat codeready linux builder for power, little endian - extended update support 8.8 ppc64le. Red hat codeready linux builder for arm 64 - extended update support 8.8 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-2023:3847 (https://access.redhat.com/errata/RHSA-2023:3847) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3847: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3847)

RESULTS:

Package	Installed Version	Required Version
kernel-core	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.15.1.el8_8
kernel-core	4.18.0-425.3.1.el8.x86_64	4.18.0-477.15.1.el8_8
kernel-core	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
python3-perf	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
kernel-tools	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
kernel-headers	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
bpftool	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
kernel-modules	4.18.0-425.3.1.el8.x86_64	4.18.0-477.15.1.el8_8
kernel-modules	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
kernel-modules	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.15.1.el8_8
kernel-tools-libs	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8
kernel	4.18.0-372.32.1.el8_6.x86_64	4.18.0-477.15.1.el8_8
kernel	4.18.0-425.3.1.el8.x86_64	4.18.0-477.15.1.el8_8
kernel	4.18.0-425.10.1.el8_7.x86_64	4.18.0-477.15.1.el8_8

3 Red Hat Update for xorg-x11-server-xwayland (RHSA-2023:2805)

CVSS: 4 CVSS3.1: 7.7 Active

QID:	241537	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-3550, CVE-2022-3551, CVE-2022-4283, CVE-2022-46340, CVE-2022-46341, CVE-2022-46342, CVE-2022-46343, CVE-2022-46344, CVE-2023-0494		
Vendor Reference:	RHSA-2023:2805		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Xwayland is an x server for running x clients under wayland...Security Fix(es): xorg-x11-server: buffer overflow in _getcountedstring() in xkb/xkb.c (cve-2022-3550). Xorg-x11-server: xkbgetkbdbyname use-after-free (cve-2022-4283). Xorg-x11-server: xtestswapfakeinput stack overflow (cve-2022-46340). Xorg-x11-server: xipassiveungrab out-of-bounds access (cve-2022-46341). Xorg-x11-server: xvdiselectvideonotify use-after-free (cve-2022-46342). Xorg-x11-server: screensaversetattributes use-after-free (cve-2022-46343). Xorg-x11-server: xichangeproperty out-of-bounds access (cve-2022-46344). Xorg-x11-server: deepcopypointerclasses use-after-free leads to privilege elevation (cve-2023-0494). Xorg-x11-server: memory leak in procxkbgetkbdbyname() in xkb/xkb.c (cve-2022-3551). 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-2023:2805 (https://access.redhat.com/errata/RHSA-2023:2805) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2805: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2805)

RESULTS:

Package	Installed Version	Required Version
xorg-x11-server-Xwayland	21.1.3-6.el8.x86_64	21.1.3-10.el8

3 Red Hat Update for gnutls (RHSA-2023:1569) CVSS: 4.2 CVSS3.1: 6.7 Active

QID:	241322	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2023-0361		
Vendor Reference:	RHSA-2023:1569		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	7.4
User Modified:	-	CVSS3.1 Temporal:	6.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06 Apr 2023 05:37:18 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 298
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Red Hat has released a security update for gnutls to fix the vulnerabilities.

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-2023:1569 (https://access.redhat.com/errata/RHSA-2023:1569) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1569: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1569)

RESULTS:

Package	Installed Version	Required Version
gnutls	3.6.16-5.el8_6.x86_64	3.6.16-6.el8_7
gnutls-dane	3.6.16-5.el8_6.x86_64	3.6.16-6.el8_7
gnutls-utils	3.6.16-5.el8_6.x86_64	3.6.16-6.el8_7

3 Red Hat Update for wayland security (RHSA-2023:2786) CVSS: 4.2 CVSS3.1: 5.9 Active

QID:	241495	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2021-3782		

Vendor Reference: RHSA-2023:2786
Bugtraq ID: -
Service Modified: 02 Jun 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS3.1 Base: 6.6
CVSS3.1 Temporal: 5.9

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

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

THREAT:
Wayland is a protocol for a compositor to talk to its clients, as well as a c library implementation of that protocol. The compositor can be a standalone display server running on linux kernel modesetting and evdev input devices, an x application, or a wayland client itself. The clients can be traditional applications, x servers (rootless or fullscreen) or other display servers...Security Fix(es): wayland: libwayland-server wl_shm reference-count overflow (cve-2021-3782). <H2></H2> 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-2023:2786 (https://access.redhat.com/errata/RHSA-2023:2786) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2786: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2786)

RESULTS:

Package	Installed Version	Required Version
libwayland-egl	1.19.0-1.el8.x86_64	1.21.0-1.el8
libwayland-cursor	1.19.0-1.el8.x86_64	1.21.0-1.el8
libwayland-server	1.19.0-1.el8.x86_64	1.21.0-1.el8
libwayland-client	1.19.0-1.el8.x86_64	1.21.0-1.el8

3 Red Hat Update for systemd (RHSA-2023:3837)

CVSS: 4.2 CVSS3.1: 7 Active

QID: 241757
Category: RedHat
Associated CVEs: CVE-2023-26604
Vendor Reference: RHSA-2023:3837
Bugtraq ID: -
Service Modified: 29 Jun 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS Base: 5.4 [1]
CVSS Temporal: 4.3

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

First Detected: 29 Jun 2023 07:27:31 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 47

Last Fixed: N/A

CVSS Environment:

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

THREAT:

The systemd packages contain systemd, a system and service manager for linux, compatible with the sysv and lsb init scripts. It provides aggressive parallelism capabilities, uses socket and d-bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount points, and implements an elaborate transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit...Security Fix(es): systemd: privilege escalation via the less pager (cve-2023-26604). Affected Products: Red Hat enterprise linux for x86_64 8 x86_64. Red hat enterprise linux for x86_64 - extended update support 8.8 x86_64. Red hat enterprise linux for ibm z systems 8 s390x. Red hat enterprise linux for ibm z systems - extended update support 8.8 s390x. Red hat enterprise linux for power, little endian 8 ppc64le. Red hat enterprise linux for power, little endian - extended update support 8.8 ppc64le. Red hat enterprise linux server - tus 8.8 x86_64. Red hat enterprise linux for arm 64 8 aarch64. Red hat enterprise linux for arm 64 - extended update support 8.8 aarch64. Red hat enterprise linux server for power le - update services for sap solutions 8.8 ppc64le. Red hat enterprise linux for x86_64 - update services for sap solutions 8.8 x86_64.. 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-2023:3837 (https://access.redhat.com/errata/RHSA-2023:3837) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3837: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3837)

RESULTS:

Package	Installed Version	Required Version
systemd-container	239-68.el8_7.2.x86_64	239-74.el8_8.2
systemd-udev	239-68.el8_7.2.x86_64	239-74.el8_8.2
systemd-libs	239-68.el8_7.2.x86_64	239-74.el8_8.2
systemd	239-68.el8_7.2.x86_64	239-74.el8_8.2
systemd-pam	239-68.el8_7.2.x86_64	239-74.el8_8.2

3 Red Hat Update for dhcp (RHSA-2023:3000)

CVSS: 4 CVSS3.1: 5.7 Active

QID:	241476	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-2928, CVE-2022-2929		
Vendor Reference:	RHSA-2023:3000		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	6.5
User Modified:	-	CVSS3.1 Temporal:	5.7
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

Asset Group:	-

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

THREAT:
The dynamic host configuration protocol (dhcp) is a protocol that allows individual devices on an ip network to get their own network configuration information, including an ip address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and isc dhcp service required to enable and administer dhcp on a network...Security Fix(es): dhcp: option refcount overflow when leasequery is enabled leading to dhcpd abort (cve-2022-2928). Dhcp: dhcp memory leak (cve-2022-2929). <H2></H2> 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-2023:3000 (https://access.redhat.com/errata/RHSA-2023:3000) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3000: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3000)

RESULTS:

Package	Installed Version	Required Version
dhcp-libs	4.3.6-48.el8_7.1.x86_64	4.3.6-49.el8
dhcp-client	4.3.6-48.el8_7.1.x86_64	4.3.6-49.el8
dhcp-common	4.3.6-48.el8_7.1.noarch	4.3.6-49.el8

2 Red Hat Update for libarchive (RHSA-2023:3018)

CVSS: 4 CVSS3.1: 8.5 Active

QID: 241480
Category: RedHat
Associated CVEs: CVE-2022-36227
Vendor Reference: RHSA-2023:3018
Bugtraq ID: -
Service Modified: 17 May 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS Base: 5.4 [1]
CVSS Temporal: 4.0

CVSS3.1 Base: 9.8
CVSS3.1 Temporal: 8.5

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
Last Fixed: N/A

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

THREAT:
The libarchive programming library can create and read several different streaming archive formats, including gnu tar, cpio, and iso 9660 cd-rom images. Libarchive is used notably in the bsdtar utility, scripting language bindings such as python-libarchive, and several popular desktop file managers...Security Fix(es): libarchive: null pointer dereference in archive_write.c (cve-2022-36227). <H2></H2>
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. Red hat codeready linux builder for ibm z systems 8 s390x.. 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-2023:3018 (https://access.redhat.com/errata/RHSA-2023:3018) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:3018: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:3018)

RESULTS:

Package	Installed Version	Required Version
libarchive	3.3.3-4.el8.x86_64	3.3.3-5.el8

2 Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1405)

CVSS: 4.2 CVSS3.1: 6.7 Active

QID:	241285	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286		
Vendor Reference:	RHSA-2023:1405		
Bugtraq ID:	-		
Service Modified:	02 Jun 2023	CVSS3.1 Base:	7.5
User Modified:	31 May 2023	CVSS3.1 Temporal:	6.7
Edited:	Yes		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 31 Mar 2023 03:22:47 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 321
Last Fixed: N/A

CVSS Environment:

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

THREAT:
Openssl is a toolkit that implements the secure sockets layer (ssl) and transport layer security (tls) protocols, as well as a full-strength general-purpose cryptography library...Security Fix(es): openssl: x.400 address type confusion in x.509 generalname (cve-2023-0286). Openssl: timing attack in rsa decryption implementation (cve-2022-4304). Openssl: double free after calling pem_read_bio_ex (cve-2022-4450). Openssl: use-after-free following bio_new_ndef (cve-2023-0215). 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-2023:1405 (https://access.redhat.com/errata/RHSA-2023:1405) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:1405: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:1405)

RESULTS:

Package	Installed Version	Required Version
openssl-devel	1.1.1k-7.el8_6.x86_64	1.1.1k-9.el8_7

openssl	1.1.1k-7.el8_6.x86_64	1.1.1k-9.el8_7
openssl-libs	1.1.1k-7.el8_6.x86_64	1.1.1k-9.el8_7

2 Red Hat Update for samba security (RHSA-2023:2987) CVSS: 4.2 CVSS3.1: 5 Active

QID:	241483	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-1615		
Vendor Reference:	RHSA-2023:2987		
Bugtraq ID:	-		
Service Modified:	01 Jun 2023	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)

Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)

Times Detected: 157

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Samba is an open-source implementation of the server message block (smb) protocol and the related common internet file system (cifs) protocol, which allow pc-compatible machines to share files, printers, and various information...Security Fix(es): samba: gnutls gnutls_rnd() can fail and give predictable random values (cve-2022-1615). <H2></H2> 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. Red hat codeready linux builder for ibm z systems 8 s390x..
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-2023:2987 (https://access.redhat.com/errata/RHSA-2023:2987) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2987: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2987)

RESULTS:

Package	Installed Version	Required Version
samba-client-libs	4.16.4-2.el8.x86_64	4.17.5-2.el8
libwbclient	4.16.4-2.el8.x86_64	4.17.5-2.el8
libsmbclient	4.16.4-2.el8.x86_64	4.17.5-2.el8
samba-common	4.16.4-2.el8.noarch	4.17.5-2.el8
samba-common-libs	4.16.4-2.el8.x86_64	4.17.5-2.el8

2 Red Hat Update for curl (RHSA-2023:2963) CVSS: 4.2 CVSS3.1: 5.3 Active

QID:	241503	CVSS Base:	5.4 [1]
Category:	RedHat	CVSS Temporal:	4.3
Associated CVEs:	CVE-2022-35252, CVE-2022-43552		

Vendor Reference: RHSA-2023:2963
Bugtraq ID: -
Service Modified: 02 Jun 2023
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

CVSS3.1 Base: 5.9
CVSS3.1 Temporal: 5.3

First Detected: 19 May 2023 04:54:09 AM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 157
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: incorrect handling of control code characters in cookies (cve-2022-35252). Curl: use-after-free triggered by an http proxy deny response (cve-2022-43552). <H2></H2> 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-2023:2963 (https://access.redhat.com/errata/RHSA-2023:2963) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
RHSA-2023:2963: Red Hat Enterprise Linux (https://access.redhat.com/errata/RHSA-2023:2963)

RESULTS:

Package	Installed Version	Required Version
curl	7.61.1-25.el8_7.1.x86_64	7.61.1-30.el8
libcurl	7.61.1-25.el8_7.1.x86_64	7.61.1-30.el8
libcurl-devel	7.61.1-25.el8_7.1.x86_64	7.61.1-30.el8

1 World-Writable Directories Should Have Their Sticky Bits Set CVSS: 0 CVSS3.1: - Active

QID: 105146
Category: Security Policy
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12 May 2023
User Modified: -
Edited: No
PCI Vuln: No
Ticket State: Closed/Fixed

CVSS Base: 0.0 [1]
CVSS Temporal: 0.0

CVSS3.1 Base: -
CVSS3.1 Temporal: -

First Detected: 14 Jul 2022 02:50:08 PM (GMT+0530)
Last Detected: 19 Jul 2023 12:11:47 AM (GMT+0530)
Times Detected: 1146
Last Fixed: N/A

CVSS Environment:

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

THREAT:
The Results section lists world-writable directories whose sticky bits are not set.

IMPACT:
N/A

SOLUTION:
It's best practice to set the sticky bit for world-writable directories.

RESULTS:
/tmp/NetBackup_8.2_CLIENTS2/Doc
/tmp/NetBackup_8.2_CLIENTS2/NBClients
/var/www/html/registering-a-new-complaint/files

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.