tenable.sc™

SMBC VA Scan Report (PDF)_2 (Scan: Adhoc_CPG_UL_20201104)

Generated on November 4, 2020 at 4:14 PM +08

Imported on November 4, 2020 at 4:14 PM +08 (Scan Result ID #2481)

Hock Chin Kok [Hock Chin Kok]
SUMITOMO MITSUI BANKING CORPORATION - SNG

Table of Contents

Introduction

Identifying vulnerable hosts in a network is only the first step in securing an organization. This report provides detailed information on the most vulnerable hosts identified on the network. The report is organized by plugin type (Active, Passive, and Compliance) and broken down by host. Each chapter focuses on a specific plugin type: active, passive, or compliance. For each type, the most vulnerable hosts and suggested steps to remediate vulnerabilities on them are detailed. ITS teams can use these chapters to understand the vulnerable hosts that could impact their network and implement the steps necessary for remediation.

Vulnerable System Index

Number of vulnerabilities per host

IP Address	NetBIOS Name	Low	Med.	High	Crit.
10.118.91.132		1	1	1	2
10.118.91.133		1	1	1	2
10.118.91.135		1	1	1	2
10.118.91.136	SNGU1VLCDG3S02\SNGU1VLCDG3S02	1	1	1	2
10.118.91.138		1	1	1	2
10.118.91.139		1	1	1	2
10.118.91.141		1	1	1	1
10.118.91.142		1	1	1	1
10.118.91.144		1	1	1	1
10.118.91.145		1	1	1	1

Number of hosts per vulnerability

Plugin	Plugin Name	Severity	Host Total
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10
14657	Red Hat Update Level	Critical	6
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10
70658	SSH Server CBC Mode Ciphers Enabled	Low	10

Detailed Findings

If there is any deviation with the requirement stated in the hardening checklist, a risk assessment with justification and mitigating measures must be provided by the System PIC / PM mentioned above. The risk assessment should be submitted to IPG for review and endorsement. As part of the security governance, IPG will perform periodic hardening review based on the criticality of the systems (i.e. Ranked of the system). JRI-ITS will generate the configuration of the IT assets and send it to IPG for performing the hardening review.

10.118.91.132

IP Address: 10.118.91.132	
Total: 288	

Count by Severity

Severity	Count
Critical	2
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
14657	Red Hat Update Level	Critical
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.133

IP Address: 10.118.91.133

Total: 288

Count by Severity

Severity	Count
Critical	2
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
14657	Red Hat Update Level	Critical
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.135

IP Address: 10.118.91.135	
Total: 289	

Count by Severity

Severity	Count
Critical	2
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
14657	Red Hat Update Level	Critical
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.136

IP Address: 10.118.91.136	
Total: 295	

Count by Severity

Severity	Count
Critical	2
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
14657	Red Hat Update Level	Critical
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.138

IP Address: 10.118.91.138	
Total: 290	

Count by Severity

Severity	Count
Critical	2
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
14657	Red Hat Update Level	Critical
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.139

IP Address: 10.118.91.139
Total: 290

Count by Severity

Severity	Count
Critical	2
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
14657	Red Hat Update Level	Critical
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.141

IP Address: 10.118.91.141	
Total: 286	

Count by Severity

Severity	Count
Critical	1
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.142

IP Address: 10.118.91.142	
Total: 286	

Count by Severity

Severity	Count
Critical	1
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.144

IP Address: 10.118.91.144	
Total: 286	

Count by Severity

Severity	Count
Critical	1
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

10.118.91.145

IP Address: 10.118.91.145	
Total: 286	

Count by Severity

Severity	Count
Critical	1
High	1
Medium	1
Low	1
Info	0

Vulnerability Details

Plugin	Plugin Name	Severity
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical
141606	RHEL 8 : kernel (RHSA-2020:4286)	High
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium
70658	SSH Server CBC Mode Ciphers Enabled	Low

Appendix

Plugin - Critical

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
14657	Red Hat Update Level	Critical	10.118.91.132	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed version : 8.1
Latest version : 8.2
```

Synopsis: The remote Red Hat server is out-of-date.

Description: The remote Red Hat server is missing the latest bugfix update package.
As a result, it is likely to contain multiple security vulnerabilities.

Solution: Apply the latest update.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease:

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.132	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
14657	Red Hat Update Level	Critical	10.118.91.133	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:
Installed version : 8.1
Latest version : 8.2

Synopsis: The remote Red Hat server is out-of-date.

Description: The remote Red Hat server is missing the latest bugfix update package.
As a result, it is likely to contain multiple security vulnerabilities.

Solution: Apply the latest update.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease:

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.133	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
14657	Red Hat Update Level	Critical	10.118.91.135	0	No

NetBIOS Name:

Plugin Text:

<u>**Plugin Output**</u>:
Installed version : 8.1
Latest version : 8.2

Synopsis: The remote Red Hat server is out-of-date.

Description: The remote Red Hat server is missing the latest bugfix update package.
As a result, it is likely to contain multiple security vulnerabilities.

Solution: Apply the latest update.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08	
Patch Publication Date: N/A	
Exploit Ease:	
Exploit Frameworks:	

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.135	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
14657	Red Hat Update Level	Critical	10.118.91.136	0	No

NetBIOS Name: SNGU1VLCDG3S02\SNGU1VLCDG3S02

Plugin Text:

Plugin Output:
Installed version : 8.1
Latest version : 8.2

Synopsis: The remote Red Hat server is out-of-date.

Description: The remote Red Hat server is missing the latest bugfix update package.
As a result, it is likely to contain multiple security vulnerabilities.

Solution: Apply the latest update.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease:

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.136	0	No

NetBIOS Name: SNGU1VLCDG3S02\SNGU1VLCDG3S02

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
14657	Red Hat Update Level	Critical	10.118.91.138	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed version : 8.1
Latest version : 8.2
```

Synopsis: The remote Red Hat server is out-of-date.

Description: The remote Red Hat server is missing the latest bugfix update package.
As a result, it is likely to contain multiple security vulnerabilities.

Solution: Apply the latest update.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease:

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.138	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
```

However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the package versions of the affected packages from this advisory. This scan is unable to rely on Red Hat's own security checks, which consider channels and products in their vulnerability determinations.

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
14657	Red Hat Update Level	Critical	10.118.91.139	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed version : 8.1
Latest version : 8.2
```

Synopsis: The remote Red Hat server is out-of-date.

Description: The remote Red Hat server is missing the latest bugfix update package.
As a result, it is likely to contain multiple security vulnerabilities.

Solution: Apply the latest update.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease:

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.139	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.141	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.142	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.144	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
```

```
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08	
Patch Publication Date: Feb 4, 2020 12:00:00 +08	
Exploit Ease: No known exploits are available	
Exploit Frameworks:	

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
133480	RHEL 8 : kernel (RHSA-2020:0339)	Critical	10.118.91.145	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Installed package kernel-4.18.0-193.14.3.el8_2 is greater than kernel-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-core-4.18.0-193.14.3.el8_2 is greater than kernel-core-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-modules-4.18.0-193.14.3.el8_2 is greater than kernel-modules-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-4.18.0-193.14.3.el8_2 is greater than kernel-tools-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-4.18.0-193.14.3.el8_2 is greater than kernel-tools-libs-4.18.0-147.5.1.el8_1.
However, according to uname -r, the current running kernel level is 4.18.0-147.el8.
This system requires a reboot to begin using the patched kernel level.

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for kernel is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

* kernel: heap overflow in mwifiex_update_vs_ie() function of Marvell WiFi driver (CVE-2019-14816)

* kernel: heap-based buffer overflow in mwifiex_process_country_ie() function in drivers/net/wireless/marvell/mwifiex/sta_ioctl.c (CVE-2019-14895)

* kernel: heap overflow in marvell/mwifiex/tdls.c (CVE-2019-14901)

* kernel: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel lacks a certain upper-bound check, leading to a buffer overflow (CVE-2019-17666)

* kernel: heap overflow in mwifiex_set_uap_rates() function of Marvell Wifi Driver leading to DoS (CVE-2019-14814)

* kernel: heap-overflow in mwifiex_set_wmm_params() function of Marvell WiFi driver leading to DoS (CVE-2019-14815)

* kernel: incomplete fix for race condition between mmget_not_zero()/ get_task_mm() and core dumping in CVE-2019-11599 (CVE-2019-14898)

* Kernel: KVM: export MSR_IA32_TSX_CTRL to guest - incomplete fix for TAA (CVE-2019-11135) (CVE-2019-19338)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* [Azure][8.1] Include patch 'PCI: hv: Avoid use of hv_pci_dev->pci_slot after freeing it' (BZ#1764635)

* block layer: update to v5.3 (BZ#1777766)

* backport xfs: fix missing ILOCK unlock when xfs_setattr_nonsize fails due to EDQUOT (BZ#1778692)

* Backport important bugfixes from upstream post 5.3 (BZ#1778693)

* LUN path recovery issue with Emulex LPe32002 HBA in RHEL 8.0 Server during storage side cable pull testing (BZ#1781108)

* cifs tasks enter D state and error out with 'CIFS VFS: SMB signature verification returned error = -5' (BZ#1781110)

* Update CIFS to linux 5.3 (except RDMA and conflicts) (BZ#1781113)

* RHEL8.0 - Regression to RHEL7.6 by changing force_latency found during RHEL8.0 validation for SAP HANA on POWER (BZ#1781114)

* blk-mq: overwirte performance drops on real MQ device (BZ#1782181)

Solution: Update the affected packages.

CVSS V3 Base Score: 9.8

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Feb 4, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin - High

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.132	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.133	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.135	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.136	0	No

NetBIOS Name: SNGU1VLCDG3S02\SNGU1VLCDG3S02

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
```

```
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.138	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2
```

```
Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.139	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2
```

```
Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.141	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
```

```
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.142	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2
```

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.144	0	No

NetBIOS Name:

Plugin Text:

<u>**Plugin Output**</u>:

Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

```
NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.
```

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
141606	RHEL 8 : kernel (RHSA-2020:4286)	High	10.118.91.145	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : bpftool-4.18.0-193.14.3.el8_2
Should be : bpftool-4.18.0-193.28.1.el8_2

Remote package installed : kernel-4.18.0-193.14.3.el8_2
Should be : kernel-4.18.0-193.28.1.el8_2

Remote package installed : kernel-core-4.18.0-193.14.3.el8_2
Should be : kernel-core-4.18.0-193.28.1.el8_2

Remote package installed : kernel-modules-4.18.0-193.14.3.el8_2
Should be : kernel-modules-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-4.18.0-193.14.3.el8_2
Should be : kernel-tools-4.18.0-193.28.1.el8_2

Remote package installed : kernel-tools-libs-4.18.0-193.14.3.el8_2
Should be : kernel-tools-libs-4.18.0-193.28.1.el8_2

Remote package installed : python3-perf-4.18.0-193.14.3.el8_2
Should be : python3-perf-4.18.0-193.28.1.el8_2

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed Red Hat repositories, but the scan lacked the permissions
```

to do so. Please rerun your scan and ensure that the scanning account
has permissions to examine the /etc/yum.repos.d/redhat.repo file.

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: The remote Redhat Enterprise Linux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:4286 advisory.

- kernel: net: bluetooth: type confusion while processing AMP packets (CVE-2020-12351)

- kernel: net: bluetooth: information leak when processing certain AMP packets (CVE-2020-12352)

- kernel: kernel: buffer over write in vgacon_scroll (CVE-2020-14331)

- kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)

- kernel: memory corruption in net/packet/af_packet.c leads to elevation of privilege (CVE-2020-14386)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Update the affected packages.

CVSS V3 Base Score: 7.8

CVSS V3 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

First Discovered: Oct 30, 2020 14:57:57 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: Oct 20, 2020 12:00:00 +08

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin - Medium

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.132	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.133	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.135	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.136	0	No

NetBIOS Name: SNGU1VLCDG3S02\SNGU1VLCDG3S02

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.138	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.139	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.141	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.142	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.144	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port	Exploit?
138374	Red Hat curl local file overwrite (CVE-2020-8177)	Medium	10.118.91.145	0	No

NetBIOS Name:

Plugin Text:

Plugin Output:

```
Remote package installed : curl-7.61.1-14.el8
Should be : curl-7.71.0-0.el8

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan is unable to rely on Red Hat's own security checks, which
consider channels and products in their vulnerability determinations.

NOTE: No fixed RHEL packages are available currently. Upstream Curl 7.71.0 fixes this vulnerability.
```

Synopsis: Red Hat Curl Local File Overwrite with -J.

Description: A local file overwrite vulnerability exists in curl 7.20.0 to and including 7.70.0 due to the -J (--remove-header-name) being allowed to be used with -i (--include). An authenticated, local attacker can exploit this, via use of a malicious server to trick curl to overwrite files on the local host.

Solution: Update curl to version 7.71.0 or later.

CVSS V3 Base Score: 5.7

CVSS V3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin - Low

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.132	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.133	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.135	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.136	22

NetBIOS Name: SNGU1VLCDG3S02\SNGU1VLCDG3S02

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.138	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.139	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
```

```
aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.141	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.142	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.144	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Severity	IP Address	Port
70658	SSH Server CBC Mode Ciphers Enabled	Low	10.118.91.145	22

NetBIOS Name:

Plugin Text:

Plugin Output:

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

aes128-cbc
aes256-cbc
```

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

CVSS V3 Base Score:

CVSS V3 Vector:

First Discovered: Oct 13, 2020 11:30:43 +08

Last Observed: Nov 4, 2020 16:14:35 +08

Patch Publication Date: N/A

Exploit Ease: No known exploits are available

Exploit Frameworks: