



VULNERABILITY MANAGEMENT

USER GUIDE

Purpose and Objectives

The main objective of Vulnerability Management is to detect, notify and where necessary remediate vulnerabilities in a timely fashion.



Table of Contents

Purpose and Objectives.....	1
1 Verizon Enterprise Center	3
2 Access to Security advisories / Vulnerability Tool	3
2.1 Main customer splash page under Repairs & Service.....	3
2.2 Service Management Dashboard Tools Dropdown	3
2.3 Security advisories POD	4
3 Customer Selection.....	4
4 Confirmed advisories.....	5
5 Potential advisories.....	5
6 Advisories and Devices View.....	6
7 Basic page navigation – Advisories View	7
8 Basic page navigation – Devices View.....	9
9 Search Functionality.....	12
10 Filter Functionality.....	13
11 Export Functionality	13
12 Record counts per page.....	14
13 Opening a Change Request – Confirmed Advisories View.....	14
14 Opening a Change Request – Confirmed Devices View	16
15 Change Request Inventory.....	17
16 Add Bulk Inventory.....	18
17 Security advisories POD.....	20
Service Assurance User Guides Library	23
General Customer Training Information.....	23
Verizon Enterprise Center	23



1 Verizon Enterprise Center

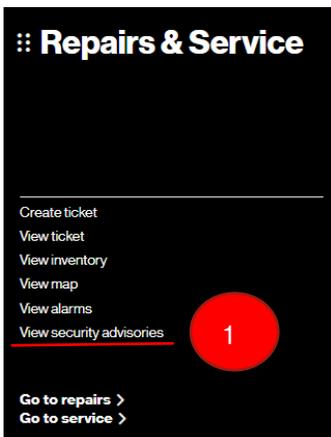
The Security advisories / Vulnerability Tool is accessed via [Verizon Enterprise Center](#). You can find the Verizon Security Advisories info-page [here](#).

2 Access to Security advisories / Vulnerability Tool

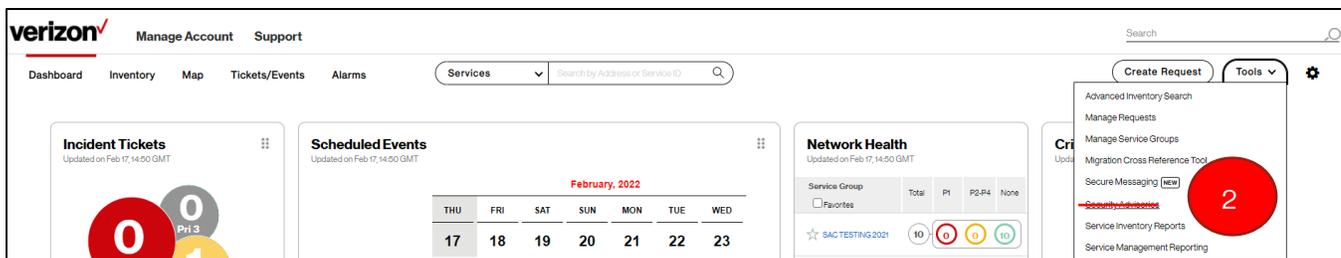
After successful login to Verizon Enterprise Center (VEC), access to the Security advisories / Vulnerability Tool can be accomplished 3 ways:

- 1) From the main customer splash page under Repairs & Service
- 2) From the Service Management Dashboard Tools Dropdown
- 3) From the Security advisories POD – (Available on the Main Splash Page or the Service Management Dashboard if added).

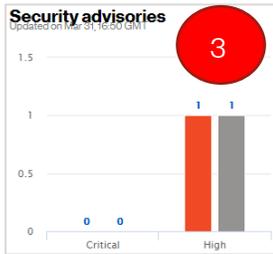
2.1 Main customer splash page under Repairs & Service



2.2 Service Management Dashboard Tools Dropdown



2.3 Security advisories POD



3 Customer Selection

Accounts listed under Customer ID are aligned to the Legal Entity Identifier (LE ID) for the customer. Some VEC users may have permissions to multiple LE IDs, thus will have as many customers listed in the Customer ID dropdown as illustrated below.

Service | Tools | Vulnerability Tool

Security advisories ⓘ

Customer ID: Managed Customer Name:

- Test Account 1
- Customer A
- Customer B
- Customer C

Based on the selected customer in the Customer ID field, associated options will be populated in the Managed Customer Name dropdown. In the example below, three Managed Customers share the same LE ID as part of Customer B.

Service | Tools | Vulnerability Tool

Security advisories ⓘ

Customer ID: Managed Customer Name:

Confirmed **Potential**

All Advisories	Critical	High
25	2	23

- Customer B (AsiaPac)
- Customer B (AsiaPac)
- Customer B (EMEA)
- Customer B (North America)



4 Confirmed advisories

Confirmed advisories have been evaluated by the Managed Services Operations team and are confirmed as impacting to the customer environment. Customer action is required to Remediate.

Confirmed advisories can be viewed by critical and high impact, or you can view both severities in the single “All Advisories” view.

Service | Tools | Vulnerability Tool Tools ▾

Security advisories ⓘ

Customer ID: Managed Customer Name:

Confirmed **Potential**

All Advisories **Critical** **High**

8 0 8 Remediate

Search by Advisory ID 🔍 ▾ ⬇ ⚙

Advisory ID	Advisory description	Customer Name	Number of devices impacted	
<input type="radio"/> CVE-2020-3405	A vulnerability in the web UI of Cisco SD-WAN vManage Software could View more		1	View
<input type="radio"/> CVE-2021-1223	Multiple Cisco products are affected by a vulnerability in the Snort View more		4	View

5 Potential advisories

Potential advisories are under evaluation by the Managed Services Operations team, but an initial triage indicates the customer is potentially impacted based on a combination of the device’s hardware model and software version. No customer action is required on a potential advisory.

Similar to confirmed advisories, potential advisories can also be viewed by critical and high impact, or you can view both severities in the single “All Advisories” view.

Service | Tools | Vulnerability Tool Tools ▾

Security advisories ⓘ

Customer ID: Managed Customer Name:

Confirmed **Potential**

All Advisories **Critical** **High**

34 4 30

Search by Advisory ID 🔍 ▾ ⬇ ⚙

Advisory ID	Advisory description	Customer Name	Number of devices impacted	
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more		1	View
CVE-2020-1979	A format string vulnerability in the PAN-OS log daemon (logd) on View more		2	View
CVE-2020-1990	A stack-based buffer overflow vulnerability in the management View more		1	View

6 Advisories and Devices View

There are two main views within the tool: Advisories View and Devices View. You can switch between the Advisories and Devices view by selecting the gear icon to the right of the search option. You can customize the columns you want to view as well as adjust the number of records per page.

Confirmed **Potential**

All Advisories 33 Critical 4 High 29

Search by Advisory ID

Advisory ID	Advisory description	Customer Name	Number of devices impacted	
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more		1	View
CVE-2020-1979	A format string vulnerability in the PAN-OS log daemon (logd) on View more		2	View



Customize table

You can choose to view the details by 'Advisories' or 'Devices'

View details by

Advisories Devices

Select columns

Customer Given Entity Name

Verizon DNS Entity Name

Serial Number

Model

OS Version

Advisories

Row settings

Items per page:



7 Basic page navigation – Advisories View

The default Advisories view contains the following columns:

- 1) Advisory ID
- 2) Advisory description
- 3) Customer name
- 4) Number of devices impacted
- 5) View

Confirmed		Potential	
All Advisories 33	Critical 4	High 29	
Advisory ID	Advisory description	Customer Name	Number of devices impacted
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more		1 View

The Advisory ID is the Common Vulnerabilities and Exposures (CVE) number assigned to the advisory.

Confirmed		Potential	
All Advisories 33	Critical 4	High 29	
Advisory ID	Advisory description	Customer Name	Number of devices impacted
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more		1 View

The Advisory description is the vendor's summary of the advisory.

Confirmed		Potential	
All Advisories 33	Critical 4	High 29	
Advisory ID	Advisory description	Customer Name	Number of devices impacted
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more		1 View

Select View more to see the full summary of the advisory.

Advisory ID	Advisory description
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more



Select View less to minimize the summary of the advisory.

Advisory ID	Advisory description
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo Alto Networks PAN-OS software allows authenticated users to inject arbitrary XML, that results in privilege escalation. This issue affects PAN-OS 8.1 versions earlier than PAN-OS 8.112 and PAN-OS 9.0 versions earlier than PAN-OS 9.0.6. This issue does not affect PAN-OS 7.1, PAN-OS 8.0, or PAN-OS 9.1 or later versions. View less

The Customer Name is the customer short name assigned in Verizon's database of record.

Confirmed		Potential	
All Advisories	Critical	High	
33	4	29	

Advisory ID	Advisory description	Customer Name	Number of devices impacted	
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more	3	1	View

The Number of devices impacted is a count of customer devices impacted by a given advisory. In the example below only 1 device is potentially impacted by CVE-2020-1975.

Confirmed		Potential	
All Advisories	Critical	High	
33	4	29	

Advisory ID	Advisory description	Customer Name	Number of devices impacted	
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more		4	1 View

The View link provides a view of the devices impacted and a reference link to additional details on the CVE.

Confirmed		Potential	
All Advisories	Critical	High	
33	4	29	

Advisory ID	Advisory description	Customer Name	Number of devices impacted	
CVE-2020-1975	Missing XML validation vulnerability in the PAN-OS web interface on Palo View more			5 View



If you select Link under References, you will be linked to the National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD) where you can gather additional information on the advisory.

Devices impacted		
Advisory ID: CVE-2020-1975		
Verizon DNS Entity name	Serial number	Severity
e022	Not Defined	HIGH
Customer Given Entity Name	Model	References
e022	VNS-SECURITY	Link
	OS version	
	9.010	

8 Basic page navigation – Devices View

The Devices view contains the following columns:

- 1) Customer Given Entity Name (not in the default view, customize columns to add)
- 2) Verizon DNS Entity Name
- 3) Serial Number
- 4) Model
- 5) OS Version
- 6) Advisories
- 7) View

Confirmed		Potential				
All Devices	Critical	High				
5	1	4				
Devices Impacted: 4						
Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories	
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High	View
e017	e017	00705	VNS-SECURITY		1High	View
e022	e022	Not Defined	VNS-SECURITY	9.010	27High/4 Critical	View
SANJOSE-SCI	e014	007	VNS-SECURITY	8.0.7	1High	View
1-4 of 4				25 Records	Go to: 1 / 1	<< 1 >>



The Customer Given Entity Name is the device name provided by the customer. This field is not in the default view and must be added. Population of this field is dependent on the customer device name being provided by the customer and the device name being added in Verizon's database.

1

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

The Verizon DNS Entity Name is the unique name given by Verizon to the device.

2

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

Serial Number is the serial number of the device.

3

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

Model is the vendor model number of the device.

4

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View



OS Version is the Operating System software currently running on the device.

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

5

The Advisories column lists the number of advisories and severity of advisories for a device. This field could display a value such as 5 High|2 Critical.

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

6

The View link provides a view of the CVEs which potentially impact the device and a reference link to additional details on the CVE.

Confirmed		Potential	
All Devices	Critical	High	
5	1	4	

Devices Impacted: 4

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

7



If you select Link under References, you will be linked to the National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD) where you can gather additional information on the advisory.

Advisory details

Verizon DNS Entity name
e022

Customer Given Entity Name
e022

Advisory ID	Date	Description
CVE-2020-2007	February 17, 2022	An OS command injection vulnerability in the management server component of PAN-OS allows an authenticated user to potentially execute arbitrary commands with root privileges. This issue affects: All PAN-OS 71 versions; PAN-OS 81 versions earlier than 8.114; PAN-OS 9.0 versions earlier than 9.0.7.
High	Customer name	
	References	Link

Advisory ID	Date	Description
CVE-2020-2010	February 17, 2022	An OS command injection vulnerability in PAN-OS management interface allows an authenticated administrator to execute arbitrary OS commands with root privileges. This issue affects: All versions of PAN-OS 71 and 8.0; PAN-OS 81 versions earlier than 8.114; PAN-OS 9.0 versions earlier than 9.0.7.
High	Customer name	
	References	Link

9 Search Functionality

Regardless of your view, Advisories or Devices, the location of the search function remains constant.

Confirmed Potential

All Devices 5 Critical 1 High 4

Devices Impacted: 4

Search by Verizon DNS Entity Name

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View
e017	e017	00705	VNS-SECURITY		1High View

However, the search functionality caters to the view you are in. In the Devices view you can “Search by Verizon DNS Entity Name” whereas in the Advisories view you can “Search by Advisory ID.”

Devices view search functionality

Search by Verizon DNS Entity Name

Advisories view search functionality

Search by Advisory ID

10 Filter Functionality

Regardless of your view, Advisories or Devices, the location of the filter function remains constant. You can customize according to your needs.

Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View

11 Export Functionality

Regardless of your view, Advisories or Devices, the location of the export function remains constant.

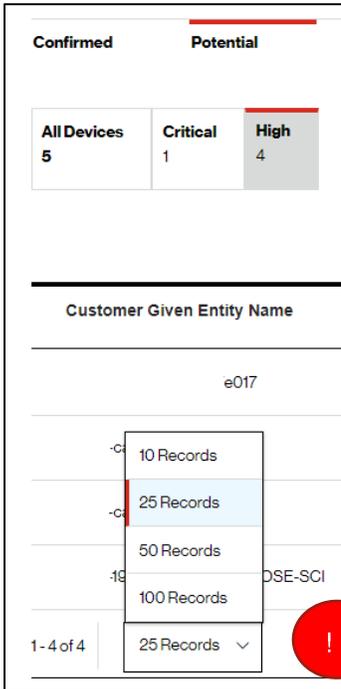
Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories
e017	e017	9VR60	VNS-ROUTING	17.3.3	1High View

The file export will contain 3 tabs.

1. Advisory View Summary – Includes a list of all advisories by State (Confirmed & Potential), Severity (Critical & High) and Number of Devices Impacted per advisory.
2. Device View Summary – Includes a list of all devices by State (Confirmed & Potential), Severity (Critical & High) and number of Advisories in total that impact the device.
3. Details – this is the raw data that is summarized in the previous mentioned summary views.

12 Record counts per page

You can view increments of 25 records per page up to 100 records. This can be modified at the lower left corner of each page within both the Advisories vs Devices View. You can also adjust the number of records per page using the Customize columns option referenced in Section 4.



13 Opening a Change Request – Confirmed Advisories View

You can open a Change Request (CR) for confirmed advisories only. One Advisory (CVE) is allowed per Change Request (CR) and all devices impacted by the selected advisory will be added to the change request (CR).

Note: It is not recommended to select an advisory that has greater than 100 devices at this time. Please leverage the device view if this scenario is applicable to your advisory. See section 14 “Bulk Inventory” as another alternative. All Change Request fields are pre-populated with the exception of the Requested Start Date/Time and Requested Completion Date/Time. You can include additional details in the Title and Objective fields if necessary.

Initiate the following steps to open a Change Request (CR):

- 1) Select the CVE you want to remediate.
- 2) Select the “Remediate” button. A new browser tab will open.
- 3) Populate additional information in the Title field (optional)
- 4) Populate additional information in the Objective field (optional)
- 5) Populate the Requested Start Date/Time (GMT) in the Change Request
- 6) Populate the Requested Completion Date/Time (GMT) in the Change Request
- 7) Submit the Change Request

Confirmed		Potential	
All Advisories	Critical	High	
8	0	8	

2
Remediate

Search by Advisory ID 🔍 📄 📌 ⚙️

Advisory ID	Advisory description	Customer Name	Number of devices impacted
<input type="radio"/> CVE-2020-3405	A vulnerability in the web UI of Cisco SD-WAN vManage Software could View more		1 View
<input checked="" type="radio"/> CVE-2021-1223	Multiple Cisco products are affected by a vulnerability in the Snort View more		4 View
<input type="radio"/> CVE-2021-1260	Multiple vulnerabilities in Cisco SD-WAN products could allow an View more		1 View

New browser tab within the Global Change Management tool.

Home > Create Request > LLC.

Customer Name: LLC.

Requested CTI: Managed Network > Vulscan > Software Vulnerability Upgrade ✎

Submitter: > @verizon.com

Summary

***Title**
Security Advisory Remediation Request

***Objective**
Request to remediate a device that is affected by a vendor released security advisory. An extended maintenance window and/or project may be required depending on the number of devices/advisories selected.

Note: An extended maintenance window and/or project may be required depending on the number of advisories that are part of the advisory you selected.

When would you like Verizon to implement your request? **Implement Anytime**

***Requested Start Date/Time (GMT)** ***Requested Completion Date/Time (GMT)**

mm/dd/yyyy hh mm mm/dd/yyyy hh mm

Submit
Save as Draft
Cancel

Home > Create Request > LLC.

✔ **Your request has been submitted.**

A new request (**Managed Network > Vulscan > Software Vulnerability Upgrade**) has been submitted for customer **LLC**

Request Number is [CR2022021722147](#) .

New Request

14 Opening a Change Request – Confirmed Devices View

You can open a Change Request (CR) for confirmed devices only. One or multiple devices can be selected. All associated CVEs for the given device(s) selected will be added to the change request (CR) for remediation.

All fields are pre-populated in the change request with the exception of the Requested Start Date/Time and Requested Completion Date/Time. You can include additional details in the Title and Objective fields if necessary.

Initiate the following steps to open a Change Request (CR):

- 1) Select the device(s) you want to remediate.
- 2) Select the “Remediate” button. A new browser tab will open.
- 3) Populate additional information in the Title field (optional)
- 4) Populate additional information in the Objective field (optional)
- 5) Populate the Requested Start Date/Time (GMT) in the Change Request
- 6) Populate the Requested Completion Date/Time (GMT) in the Change Request
- 7) Submit the Change Request

Confirmed		Potential					
All Devices	Critical	High					
12	0	12					
Devices Impacted: 12			Search by Verizon DNS Entity Name <input type="text"/>				
<input type="checkbox"/>	Customer Given Entity Name	Verizon DNS Entity Name	Serial Number	Model	OS Version	Advisories	
<input type="checkbox"/>	e004	e004	ESP_NULL	VNS-SDWAN	20.3.4	1High	View
<input checked="" type="checkbox"/>	9e004	e004	db187a02-	VNS-SDWAN	20.3.3	1High	View
<input checked="" type="checkbox"/>	7e009	e009	823	VNS-SDWAN	18.4.3	2High	View
<input checked="" type="checkbox"/>	e016	e016	B79	VNS-SDWAN	19.2.3	6High	View

New browser tab within the Global Change Management tool.

Home > Create Request > Verizon LLC.

Customer Name: LLC

Requested CTI: Managed Network > Vulscan > Software Vulnerability Upgrade

Submitter: > @verizon.com

Summary

***Title**
Security Advisory Remediation Request

***Objective**
Request to remediate a device that is affected by a vendor released security advisory. An extended maintenance window and/or project may be required depending on the number of devices/advisories selected.

Note: An extended maintenance window and/or project may be required depending on the number of advisories that are part of the advisory you selected.

5

6

7

When would you like Verizon to implement your request? Implement Anytime

* Requested Start Date/Time (GMT)

* Requested Completion Date/Time (GMT)

Submit **Save as Draft** **Cancel**

Home > Create Request > LLC.

✓ Your request has been submitted.

A new request (**Managed Network > Vulscan > Software Vulnerability Upgrade**) has been submitted for customer **LLC**

Request Number is **CR2022021722147** .

New Request

15 Change Request Inventory

Irrespective of the view (Advisory or Device) that you open the Change Request (CR) from, the inventory you selected within the Security advisory tool will be attached as an Excel file under Inventory Details.

Inventory Details

Managed Network Customer:

[Add Inventory](#) -OR- [Add Bulk Inventory](#)

Actions	Type	Attachment Name	Creation Date (GMT)
		Vulscan-DeviceList-2022-02-17 171847.xls	2022-02-17 17:18:48

Per the example below, three devices were selected for remediation. Configuration items “e009” and “e016” have more than 1 advisory that will be remediated as part of the Change Request.

	A	B	C	D
1	configuration item	configuration item type		advisories
2	e009	ENTITY		CVE-2020-3405,CVE-2021-1262
3	e004	ENTITY		CVE-2021-1262
4	e016	ENTITY		CVE-2021-1260,CVE-2021-1261,CVE-2021-1262,CVE-2021-1263,CVE-2021-1298,CVE-2021-1299
5				

Following submission of the Change Request, the inventory is visible in two places.

- 1) The Details Tab of the CR under Configuration Items
- 2) The Attachments tab

CR2022021722147 (Normal) State: Open Status: Submitted

Submit Assess Plan Approve Implement Verify Close

DETAILS COMMENTS CONTACTS ATTACHMENTS RELATED REQUEST & ORDERS MILESTONE & ACTIVITIES NOTIFICATIONS

Request CTE: Managed Network > Vulscan > Software Vulnerability Upgrade

Title: Security Advisory Remediation Request

Submitter: > @verizon.com ✉

Customer Name: LLC. Management Domain: d43

Customer Reference Number: NA Customer Reference System: NA

Management Center (TMG): MCCMS Support Team (TOG): STAS

Review Duration (hh:mm): Implementation Duration (hh:mm):

Objective: Request to remediate a device that is affected by a vendor released security advisory. An extended maintenance window and/or project may be required depending on the number of devices/advisories selected.

Configuration Items

#	DNS Entity Name	DNS Short Name	Entity Host Name	Equipment Type	Model	IP Address
1	e009	27	e009	SD WAN VM	VNS-SDWAN	108
2	e004	259	e004	SD WAN VM	VNS-SDWAN	166
3	e016	274	e016	SD WAN VM	VNS-SDWAN	108

1

CR2022021722147 (Normal) State: Open Status: Submitted

Submit Assess Plan Approve Implement Verify Close

DETAILS COMMENTS CONTACTS ATTACHMENTS RELATED REQUEST & ORDERS MILESTONE & ACTIVITIES NOTIFICATIONS

Category: General Sub Category: Document Access Type: Customer

Description:

(A Maximum of 10 files with file size of 10MB per file is allowed.) [Browse Files](#)

No	Type	Attachment Name	Description	Access Type	Creation Date (GMT)
1		Vulscan-DeviceList-2022-02-17 171847.xls		Customer	2022-02-17 17:26:05

2

16 Add Bulk Inventory

If the advisory you selected to “Remediate” has more than 100 devices, you have the option to remove devices from the Change Request Inventory prior to submission of the request via the “Add Bulk Inventory” option within the Global Change Management Tool. The following steps apply.

- 1) Under the Inventory Details section, open (download) the attachment under Attachment Name
- 2) Open the spreadsheet attachment
- 3) The original file will display all devices impacted by the CVE you selected to remediate. In the example below, eight (8) devices are part of the original list of devices.
- 4) Delete the applicable rows from the spreadsheet. In the example below, rows 8 and 9 were deleted from the original list.
 - a. **Note:** *Do not make any other alterations to the spreadsheet else the Change Request will fail.*
- 5) Save the updated file to your local machine
- 6) Select the trash can option to delete the original inventory file.
- 7) A pop up will ask you if you want to delete the file. Select “Yes”

8) Another pop up will then ask you to upload the new file. Select “Choose File” and select the file that you saved to your local machine. The new file will be uploaded to your Change Request. If all required fields in the Change Request have been populated, you may submit at this time. When opening the newly submitted Change Request, the number of Configuration Items will make the number in the spreadsheet you uploaded.

9)

Inventory Details

Managed Network Customer:

[Add Inventory](#) -OR- [Add Bulk Inventory](#)

Actions	Type	Attachment Name	Creation Date (GMT)
🗑️	📄	Vulscan-DeviceList-2022-03-02 123008.xls	2022-03-02 12:30:08

Inventory Details

Managed Network Customer:

[Add Inventory](#) -OR- [Add Bulk Inventory](#)

Actions	Type	Attachment Name	Creation Date (GMT)
🗑️	📄	Vulscan-DeviceList-2022-03-02 123413.xls	2022-03-02 12:34:13

+ Other Details

📄 Vulscan-DeviceList-...xls [Show all](#)

#	A	B	C	D	E
1	configuration item	configuration item type		advisories	
2	099e004	ENTITY		CVE-2021-1262	
3	299e004	ENTITY		CVE-2021-1262	
4	267e009	ENTITY		CVE-2021-1262	
5	303e004	ENTITY		CVE-2021-1262	
6	267e021	ENTITY		CVE-2021-1262	
7	699e001	ENTITY		CVE-2021-1262	
8	699e004	ENTITY		CVE-2021-1262	
9	267e016	ENTITY		CVE-2021-1262	
10					
11					
12					

4

	A	B	C	D	E
1	configuration item	configuration item type		advisories	
2	099e004	ENTITY		CVE-2021-1262	
3	299e004	ENTITY		CVE-2021-1262	
4	267e009	ENTITY		CVE-2021-1262	
5	303e004	ENTITY		CVE-2021-1262	
6	267e021	ENTITY		CVE-2021-1262	
7	699e001	ENTITY		CVE-2021-1262	
8					
9					
10					
11					

Inventory Details

Managed Network Customer:

[* Add Inventory](#) -OR- [* Add Bulk Inventory](#)

Actions	Type	Attachment Name	Creation Date (GMT)
		Vulscan-DeviceList-2022-03-02 123008.xls	2022-03-02 12:30:08

Confirm

Are you sure you want to delete "Vulscan-DeviceList-2022-03-02 124455.xls" ?

Add Bulk Inventory

Attachments

(Up to 1 file(s), each with a maximum size of 10MB is allowed. Accepted file formats are .xls,.xlsx,.csv)

Please Wait...

Uploading your file

17 Security advisories POD

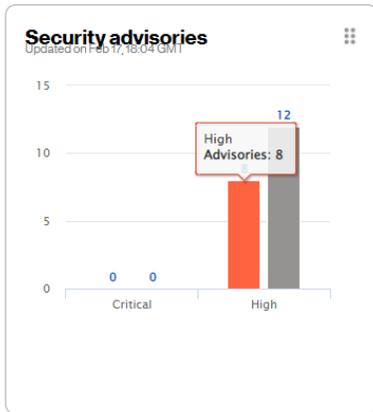
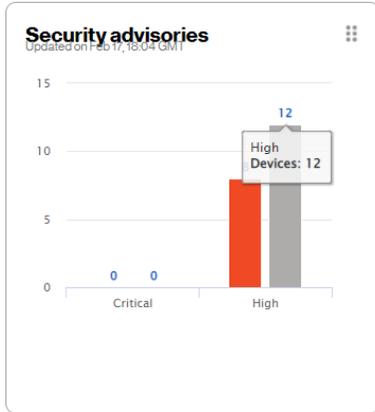
The Security advisories POD provides a quick illustration of the following:

- 1) Number of Devices confirmed to be impacted by a High severity advisory
- 2) Number of Advisories confirmed as High severity
- 3) Number of Devices confirmed to be impacted by a Critical severity advisory
- 4) Number of Advisories confirmed as Critical severity

The first example below illustrates that 12 devices are impacted by a High severity advisory.

The second example below illustrates that there are 8 High severity advisories.

Per both examples below, there are no Critical advisories and/or devices impacted by a Critical advisory.





Service Assurance User Guides Library

Documents can be found on the [Service Assurance User Guides](#) page.
The latest version of this document can be always found [here](#).

General Customer Training Information

Go to our [Customer Training Portal](#)* to enroll in training or to download other user and reference guides.
*Registration is required

Verizon Enterprise Center

The [Verizon Enterprise Center](#) portal is an easily accessible tool that supports you in dealing with Repair related technical issues via repair tickets, as well as with Invoice inquiries and Account Management requests, offering an alternative to emails and phone calls.

Getting started on Verizon Enterprise Center

Introduction to Verizon Enterprise Center and information on how to register can be found on the Guides & Tutorials page [here](#).



© 2023 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. Microsoft and Excel are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.