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

Vulnerability Scope & Summary ........................................................................................................... 2
Risk Scoring ........................................................................................................................................... 2
Risk Assessment ................................................................................................................................. 3
What Verizon Does ............................................................................................................................ 3
Update your Security Vulnerability Notification Contact ............................................................... 3
Vulnerability Remediation Steps ......................................................................................................... 4
Understanding Remediation ............................................................................................................... 5
References .............................................................................................................................................. 6
Appendix ............................................................................................................................................... 6
Customer Training and User Guides ............................................................................................... 7
Vulnerability Scope & Summary

Vulnerability Management is applicable to EMEA and APAC customers with Managed WAN and Managed LAN.

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

Vulnerabilities in the Verizon managed services environment consist of software flaws and configuration errors that are present in fully managed Verizon devices such as routers, switches, WAN accelerators, wireless access points etc.

When software is flawed or has errors, it is no longer secure and can then become vulnerable to hackers.

Subject to any contractual restrictions, Verizon will proactively assess and notify you via email notifications if any of your managed devices are impacted by a security vulnerability giving you the opportunity to remediate if required.

Risk Scoring

Vulnerabilities are assigned a risk level to accurately determine risk.

They are rated according to their severity by the Common Vulnerability Scoring System (CVSS).

CVSS is a vendor-neutral, industry standard that conveys vulnerability severity and helps determine urgency and priority of response. It overcomes the problem of multiple, incompatible scoring systems and can be used to score vulnerabilities across all vendors and system types.

Verizon’s notification (see Appendix for an example) contains a link to the Vendor vulnerability announcement which includes detailed vulnerability assessment information and two ratings:

- **CVSS Base Score**: Represents the intrinsic and fundamental characteristics of vulnerability that are constant over time and user environments.
- **CVSS Temporal Score**: Represents the characteristics of vulnerability that change over time but not among user environments.

**Please Note**: Many vulnerability notifications will have no impact on the confidentiality or integrity of your data.
Risk Assessment

Confidentiality and integrity security breaches can be a challenge to identify, as it is difficult to determine if information has been accessed or changed as it may go undetected over a long period of time.

Vulnerabilities which impact availability may be easier to identify, since there would be a loss of service when the vulnerability is exploited. Example: A denial of service attack, which causes a router reload, resulting in a loss of service.

It is important to understand the importance of data confidentiality and data integrity, in addition to the impact of any downtime that may be required to remediate vulnerability before deciding the best response.

You should balance the vulnerability risk versus the:

- Service downtime required to remediate.
- Potential additional upgrade costs (i.e. device memory upgrade) required to support the vulnerability remediation.

What Verizon does

Verizon proactively scans managed customer network devices to determine if they are impacted by vendor security vulnerability announcements. This excludes end user PC’s and servers or any other customer owned network equipment as well as devices that have been requested to be removed from automatic vulnerability scanning.

After a vendor announces vulnerability, it is reviewed by Verizon to identify the managed devices impacted by vulnerabilities.

Your “Security Vulnerability Notification” contact as recorded in Verizon’s contact databases will be automatically notified by email if any managed devices are impacted by vulnerability:

- For security reasons, the email notification does not list the impacted devices
- The notification is sent once, there is a notification email for each identified vulnerability.
- A change request is required to obtain a list of impacted devices

Update your Security Vulnerability Notification Contact

It is important your “Security Vulnerability Notification” contact is kept up to date and must include at least one valid customer email address. It is possible to add additional security vulnerability contacts e.g., Your Verizon Technical Service Manager, Client Service Manager, a second customer contact etc.

To add or amend your Security Vulnerability Notification Contact, you should raise a request via the Global Change Management (GCM) system on the Verizon Enterprise Center portal.

Select the Category, Type and then use the dropdown to select the Item ‘Modify Customer Location Information’.
Enter the Summary of Change as ‘Security Vulnerability Notification POC’.

Add the Change Description ‘Please add/change the security notification POC and include the name, email and telephone number’, see the example screenshot below.

Vulnerability Remediation Steps

To obtain a list of impacted devices, you should formally request a “Software Vulnerability Assessment” Change Request via Change Management on the Verizon Enterprise Center portal. A single change request is sufficient to obtain a report of all vulnerabilities, even if multiple vulnerability notification emails are received.

The Verizon Engineer will produce the following documentation and attach it to the Change Request:

- Completed Vulnerability Assessment Report

It is important to understand the vulnerability before requesting the remediation (upgrade) because:

- The upgrade may cause service downtime
- The upgrade may require hardware device upgrades that need to take place first

If you wish to have the vulnerability remediated, you should raise a “Software Vulnerability Upgrade” via Change Management on the Verizon Enterprise Center portal and attach the completed Software Vulnerability Upgrade Form.
Understanding Remediation

Remediation typically requires a simple configuration change or a software upgrade:

- Remediation action will only be performed if the network device meets the minimum hardware and software requirements

If remediation action requires additional resource e.g. an additional software license, a memory upgrade or replacement of end of life hardware etc. this will have a financial impact and will therefore be referred to the account team to discuss with you further.

Verizon will not implement additional resource (additional software license, memory upgrade, hardware replacement) without a formal Service Order Form for a network upgrade.

Necessary steps are taken to ensure remediation actions have a minimal impact on network availability. However, all changes have an element of risk involved and this risk must be considered before submitting the “Software Vulnerability Upgrade” change request.

Remediation actions always have some element of risk involved for the service.

Remediation action can be scheduled for each change within one of the fixed three maintenance windows listed below:

- 07.00- 15.00 GMT Monday – Friday
- 15.00- 23.00 GMT Monday – Friday
- 23.00- 07.00 GMT Monday – Friday
References

Cisco Vulnerability Notification Example:

CVSS Information

Appendix

This notice is regarding the following network names: Misco Project Lab Solutions

A security evaluation by Verizon indicates that some of your managed network elements may be impacted by a vulnerability listed below. The actual vulnerability risk depends upon a number of factors including: the version of operating system currently running on the network hardware.

- The network design.
- The current running configuration.

Your individual security policy may require you to conduct a further review, analysis, and remediation. If you feel that this vulnerability requires further assistance, please open a Vulnerability Assessment change request via the Verizon Enterprise Center (https://enterprisecenter.verizon.com/) and Verizon will provide further details of vulnerabilities potentially impacting your network.

Since the assessment requires reviewing a large amount of data, your request may take longer to complete than a standard change request.

CISCO IOS Software Network Address Translation Vulnerabilities.
Advisory ID: cisco-sa-20110326-net
For Additional details:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110326-net

Please note: If you are the not the correct contact for notifications of this type, please have the "Security Vulnerability Notification" contact record updated to ensure the correct person within your organisation is notified.

Regards,
Verizon Managed Services
Customer Training and User Guides

Service Assurance User Guides

Documents can be found on the Service Assurance User Guides page.

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 offers customers the possibility of raising inquiries and managing different requests online.

What is it for?

The Verizon Enterprise Center portal supports customers with Repair related technical issues via repair tickets as well as customers with Invoice inquiries and Account Management requests, offering an alternative to emails and phone calls.

Related documents

Related documents and guides can be found on the Verizon Enterprise Center Commercial User Guides* page (follow the menu path User/Reference Guides > Verizon Enterprise Center).

*Registration is required