DigInv

Audit report

2022-06-17

Summary

DigInv performed an audit on 2022-06-17 of the network device detailed in the scope.The audit consisted of the following components:

- a best practice security audit (Part 2)
- a software vulnerability audit report (Part 3)

scope

	Name	Device	OS
0	R1	router	12.4

Security Audit Summary

DigInv performed a security audit of the device detailed in the scope and identified 3 security-related issues. Each of the issues identified is described in greater detail in the main body of this report.

Contents

1. Your Report

1.1 Introduction

This report was produced by DigInv on 2022-06-17. This report is comprised of the following sections:

- a security audit section which details any identified security-related issues. Each security issue identified includes details of what was found together with the impact of the issue, how easy it would be for an attacker to exploit and a recommendation. The recommendations may include alternatives and, where relevant, the commands to resolve the issue;

- a software vulnerability audit section that provides a comparison of the device software versions against a database of known vulnerabilities. In addition to a brief description, each potential vulnerability includes a score and references to more specific information provided by the device manufacturers and third parties;
- a configuration report which details the configuration settings of all the audited devices in an easy to read format. The configuration settings are divided in to report sub-sections which group related settings together and provide additional information about their purpose;

2 Security Audit

DigInv performed a security audit on 2022-06-17 of the device detailed in the Table below.

	Device	Name	OS
0	R1	router	12.4

2.1.1 Security Issue Overview

Each security issue identified by DigInv is described with a finding, the impact of the issue, how easy it would be for an attacker to exploit the issue and a recommendation.

Issue Finding

The issue finding describes what DigInv identified during the security audit. Typically, the finding will include background information on what particular configuration settings are prior to describing what was found.

Issue Impact

The issue impact describes what an attacker could achieve from exploiting the security audit finding. However, it is worth noting that the impact of an issue can often be influenced by other configuration settings, which could heighten or partially mitigate the issue. For example, a weak password could be partially mitigated if the access gained from using it is restricted in some way.

Issue Ease

The issue ease describes the knowledge, skill, level of access and time scales that would be required by an attacker in order to exploit an issue. The issue ease will describe, where relevant, if any Open Source or commercially available tools could be used to exploit an issue.

Issue Recommandation

Each issue includes a recommendation section which describes the steps that DigInv recommends should be taken in order to mitigate the issue. The recommendation includes, where relevant, the commands that can be used to resolve the issue.

2.1.2 Rating System Overview

Each issue identified in the security audit is rated against both the impact of the issue and how easy it would be for an attacker to exploit. The fix rating provides a guide to the effort required to resolve the issue. The overall rating for the issue is calculated based on the issue's impact and ease ratings.

Impact Rating

An issue's impact rating is determined using the criteria outlined in the Table below.

	Rating	Description
0	CRITICAL	These issues can pose a very significant security threat. The issues that have a critical impact are typically those that would allow an attacker to gain full administrative access to the device. For a firewall device, allowing all traffic to pass through the device unfiltered would receive this rating as filtering traffic to protect other devices is the primary purpose of a firewall.
1	HIGH	These issues pose a significant threat to security, but have some limitations on the extent to which they can be abused. User level access to a device and a DoS vulnerability in a critical service would fall into this category. A firewall device that allowed significant unfiltered access, such as allowing entire subnets through or not filtering in all directions, would fall into this category. A router that allows significant modification of its routing configuration would also fall into this category.

2	MEDIUM	These issues have significant limitations on the direct impact they can cause. Typically, these issues would include significant information leakage issues, less significant DoS issues or those that provide significantly limited access. An SNMP service that is secured with a default or a dictionary-based community string would typically fall into this rating, as would a firewall that allows unfiltered access to a range of services on a device.
3	LOW	These issues represent a low level security threat. A typical issue would involve information leakage that could be useful to an attacker, such as a list of users or version details
4	INFORMATIONAL	These issues represent a very low level of security threat. These issues include minor information leakage, unnecessary services or legacy protocols that present no real threat to security

Ease Rating

An issue's ease rating is determined using the criteria outlined in the Table below.

	Rating	Description
0	TRIVIAL	The issue requires little-to-no knowledge on behalf of an attacker and can be exploited using standard operating system tools. A firewall device which had a network filtering configuration that enables traffic to pass through would fall into this category.
1	EASY	The issue requires some knowledge for an attacker to exploit, which could be performed using standard operating system tools or tools downloaded from the Internet. An administrative service without or with a default password would fall into this category, as would a simple software vulnerability exploit.
2	MODERATE	The issue requires specific knowledge on behalf of an attacker. The issue could be exploited using a combination of operating system tools or publicly available tools downloaded from the Internet.
3	CHALLENGE	A security issue that falls into this category would require significant effort and knowledge on behalf of the attacker. The attacker may require specific physical access to resources or to the network infrastructure in order to successfully exploit the vulnerability. Furthermore, a combination of attacks may be required.
4	N/A	The issue is not directly exploitable. An issue such as enabling legacy protocols or unnecessary services would fall into this rating category.

Fix Rating

An issue's fix rating is determined using the criteria outlined in the Table below.

	Rating	Description
0	INVOLVED	The resolution of the issue will require significant resources to resolve and is likely to include disruption to network services, and possibly the modification of other network device configurations. The issue could involve upgrading a device's OS and possible modifications to the hardware.
1	PLANNED	The issue resolution involves planning, testing and could cause some disruption to services. This issue could involve changes to routing protocols and changes to network filtering.
2	QUICK	The issue is quick to resolve. Typically this would just involve changing a small number of settings and would have little-to-no effect on network services.

Global Audit

1. UDP Small Services Enabled

Overall:HIGH
Impact:High

Ease:Trivial
Fix:Quick

observation

Some devices and platforms provide a collection of simple User Datagram Protocol (UDP) network services, which are also sometimes referred to Fix: Quick as small services. These services provide little functionality and are rarely used and they typically include: Echo (defined in RFC 862) returns any data sent to it back to the connecting client; Discard (defined in RFC 863) ignores any data sent to it by a connecting client; Chargen (defined in RFC 864) generates printable characters which are returned to the connecting client. DigInv determined that the UDP small servers were enabled

impact

- An attacker could use the UDP small servers as part of a DoS attack. UDP is a connection-less protocol and an experienced attacker could forge network packets to use the echo and chargen services to increase the network traffic and system utilization of devices offering the services. Additionally, each running service increases the chances of an attacker being able to identify the device and successfully compromise it. Although not as significant, some of the services may provide an attacker with simple information that could then be used as part of a targeted attack against the system.

ease

Tools that can be used to connect to these services are installed by default on some systems or can be downloaded from the Internet.

recommandation

- DigInv recommends that the UDP small servers should be disabled.

```
no service udp-small-servers
```

2. No HTTP Server Session Timeout

Overall:HIGH
Impact:High
Ease:Easy
Fix:Quick

observation

The HTTP server session timeout setting is used to determine if a web session is no longer being used, enabling a device to determine when a connection can be automatically disconnected. A HTTP server session could become unused if an administrator has not properly terminated a connection and remains authenticated, such as when a user does not click on a logout button. The session could also become unused if the user leaves their computer unattended without terminating the session.

impact

- If an attacker was able to access a system using an authenticated session that is no longer being used, the attacker would be able to perform information gathering, configuration and other malicious activities under the context of the previous authenticated user. The level of access could potentially be at an administrative level.

ease

To exploit this issue an attacker would first have to identify a working HTTP server session, possibly prior to it becoming unused by the user, and then be able to control that web session. This may be as simple as using the users computer whilst they are away, otherwise the attacker may have to exploit a weakness in the protocol or perform a man-in-the-middle attack. The man-in-the-middle attack could be performed using a proxy server, but a user could become suspicious if the session is using Hypertext Transfer Protocol over SSL (HTTPS) and the web browser provides the user with a certificate warning.

recommandation

- DigInv recommends that a HTTP server session timeout period of 10 minutes should be configured.

```
ip http timeout-policy idle seconds life seconds requests number
```

3. No Inbound TCP Connection Keep-Alives

Overall:HIGH
Impact:High
Ease:Easy
Fix:Quick

observation

The keep-alive messages are used to determine if a connection is active or has become orphaned and is no longer used. Depending on the result, the device can reclaim resources allocated to inbound connections that have become orphaned. Connections to a device could become orphaned if a connection becomes disrupted or if the client has not properly terminated a connection.

impact

- An attacker could attempt a DoS attack against a device by exhausting the number of possible connections. To perform this attack, the attacker could keep requesting new connections to the device and spoof the source IP addresses. This would then prevent any new legitimate connections to the device from being made as the device awaits the completion of the connection attempts that have already been initiated. This attack would prevent both users and administrators from connecting to the device.

ease

Tools can be downloaded from the Internet that are capable of opening a large number of TCP connections without correctly terminating them.

recommandation

- DigInv recommends that TCP keep alive messages should be sent to detect and drop orphaned connections from remote systems.

```
service tcp-keepalives-in
```

4. IP Classless

Overall:HIGH
Impact:High
Ease:Trivial
Fix:Quick

observation

Classless routing is enabled by default on Cisco routers. If a router has classless routing enabled and it receives a network packet for which there is no configured route, the router will forward the packet to the best destination. With classless routing disabled, the router would discard any network traffic for which no route is defined. DigInv determined that classless routing was enabled

impact

- Network traffic that should not be routed by the router may be routed when classless routing is enabled.

ease

N/A

recommandation

- DigInv recommends that, if possible, classless routing be disabled. Classless routing can be disabled with the following command:

```
no ip classless
```

5. AUX Port Not Disabled

Overall:MEDIUM
Impact:High
Ease:Challenging
Fix:Quick

observation

The Auxilary (AUX) port's primary purpose is to provide a remote administration capability. With a modem connected to the AUX port, a remote administrator could dial into the device in order to perform remote administration. As an extra layer of security, some devices can be configured with a callback facility. The callback facility, if configured, drops any incoming calls and dials the network administrator back.

impact

- If an attacker is able to dial in and connect to the device remotely using the AUX port, the attacker could perform a brute-force attack against the authentication mechanism in order to gain remote administrative access. If a malicious user was able to gain physical access to a device where the AUX port had not been disabled, they could attach a modem in order to perform an attack from a remote location. If a callback facility has not been configured, then the device would not drop incoming calls and attempt to dial the network administrators phone number.

ease

In order to successfully exploit this issue, the attacker would require a modem to be attached to the AUX port. If a modem is already attached, an attacker could discover the modem's telephone number during a war-dial. However, even though a number of war dial tools are available on the Internet, a war dial is more likely to be discovered due to the number of telephones which would be called in an office.

recommandation

- DigInv recommends that, if not required, the AUX port should be disabled. If the AUX port is required and the device supports callback then DigInv suggests that the callback facility should be configured as an additional level of protection.

```
transport input none login local no exec
```

6. No HTTP Service Network Access Restrictions

Overall:MEDIUM
Impact:Medium
Ease:Trivial
Fix:Quick

observation

HTTP (RFC 2616) provides web-based services, such as information services, network device administration and other potentially sensitive services. HTTP provides no encryption of the connection between the client and server including any authentication and data transfer. HTTPS, which is HTTP over Secure Sockets Layer (SSL)/TLS, is used to provide cryptographically secure web-based connection. Network access to the HTTP service can be restricted by specifying those hosts that are allowed to access the service and thereby denying access to all other network host addresses.

impact

- Without management host address restrictions an attacker, or malicious user, with authentication credentials would be able to connect to the HTTPS service, logon and access the functionality and information provided for that user. If an attacker does not have authentication credentials they could attempt a brute- force attack in order to identify valid credentials. Additionally, if there is a vulnerability with the service then allowing anyone to connect to the service could enable an attacker to exploit the vulnerability.

ease

With no HTTP network host access restrictions an attacker would not be prevented from connecting to the service. Furthermore, web browsers and other web- based client tools are included as standard with most operating systems. Alternative web service tools are available on the Internet, together with vulnerability exploit code, enumeration and brute-force tools.

recommandation

- DigInv recommends that access to the HTTP service should be restricted to only those network hosts that require access.

```
ip http access-class acl-number
```

7. Service Password Encryption Disabled

Overall:LOW
Impact:Medium
Ease:Challenging
Fix:Quick

observation

Cisco service passwords are stored by default in their clear-text form rather than being encrypted. However, it is possible to have these passwords stored using the reversible Cisco type-7 encryption. DigInv determined that the Cisco device Router was not running the password encryption service that helps provide a basic level of encryption to passwords that otherwise would be stored in clear-text.

impact

- If a malicious user were to see a Cisco configuration that contained clear-text passwords, they could use the passwords to access the device. However, an attacker who had access to a Cisco configuration file would easily be able to reverse the passwords.

ease

Even though it is trivial to reverse Cisco type-7 passwords, they do provide a greater level of security than clear-text passwords. Tools are widely available on the Internet that reverse Cisco type-7 passwords.

recommandation

- DigInv recommends that the Cisco password encryption service be enabled. The Cisco password encryption service can be started with the following Cisco IOS command:

```
service password-encryption
```

8. CDP enabled

Overall:LOW
Impact:Low
Ease:Easy
Fix:Quick

observation

CDP is a proprietary protocol that was developed and is primarily used by Cisco. A CDP enabled device can be configured to broadcast. CDP packets on the network enabling network management applications and CDP aware devices to identify each other. CDP packets include information about thesender, such as OS version and IP address information.

impact

- CDP packets contain information about the sender, such as hardware model information, operating system version and IP address details. This information would give an attacker valuable information about the device. The attacker could then use this information as part of a targeted attack.

ease

CDP packets are broadcast to an entire network segment. The attacker or malicious user would require access to a network segment on which the CDP packets are broadcast and network monitoring software. A wide variety of network monitoring, packet capture and analysis tools can be downloaded from the Internet.

recommandation

- DigInv recommends that, if not required, CDP should be disabled. In some configurations with IP phones, deployed using either Auto Discovery or Dynamic Host Configuration Protocol (DHCP), the CDP service may need to be enabled. However, if the device supports disabling CDP on individual interfaces, then DigInv recommends that it should be disabled on all the interfaces where it is not required.

```
no cdp run
```

9. VTP Was In Server Mode

Overall:LOW
Impact:Low
Ease:Moderate
Fix:Planned

observation

VTP was developed by Cisco to assist with the management of VLANs over multiple devices. The protocol enables the addition, renaming and deletion of VLANs on a single switch to be propagated to other network switches in the same VTP domain. A device in VTP server mode will transmit VTP packets containing VLAN information. If a device in VTP client mode in the same domain receives a VTP network packet with a higher revision number the changes will be applied. DigInv determined that VTP was in server mode.It is worth mentioning that although the VTP was found to be in server mode(adefault setting), no VTP domain was configured. However, there have been instances where a device in this configuration have had their VTP domain setremotely from other networked devices.

impact

- An attacker could determine the VLAN configuration by capturing VTP packets sent from the device and VTP packets are not encrypted, even when a password is specified. The attacker could then use the VLAN information or password as part of a targeted attack.

ease

Tools that are capable of capturing network packets are available on the Internet and installed by default on some OS.

recommandation

- DigInv recommends that, if not required, VTP should be disabled or placed in transparent mode, even if no VTP domain has been configured.

```
vtp transparent vtp mode transparent
```

10. IP Source Routing Was Enabled

Overall:LOW
Impact:Low
Ease:Moderate
Fix:Quick

observation

TCP/IP packets can contain source route information, this can enable a packet to define its own route through a network rather than using a route defined by static routes or routing protocols. The source route option functionality was defined in RFC 791. Many network filtering and routing devices include facilities that enable them to ignore the source route defined in a packet or block the packets entirely. DigInv determined that IP source routing was enabled

impact

- IP source routing can allow an attacker to specify a route for a network packet to follow, possibly to bypass a Firewall device or an Intrusion Detection System (IDS). An attacker could also use source routing to capture network traffic by routing it through a system controlled by the attacker.

ease

An attacker would have to control either a routing device or an end point device in order to modify a packets route through the network. However, tools can be downloaded from the Internet that would allow an attacker to specify source routes. Tools are also available to modify network routing using vulnerabilities in some routing protocols.

recommandation

- DigInv recommends that IP source routing information contained in network packets should be ignored.

```
no ip source-route
```

11. Warning In Pre-Logon Banner

Overall:LOW
Impact:Low
Ease:N/A
Fix:Quick

observation

Logon banner messages are an important, but often overlooked, part of a secure configuration. Logon banner messages can provide connecting users with important information and warn against unauthorized access.

impact

- A carefully worded warning message could deter a casual attacker or malicious user, but not a determined attacker. However, it would be more difficult to prove any intent without a message warning against unauthorized access if any legal action were to be taken against an attacker.

ease

An attacker would not be presented with a carefully worded legal warning prior to attempting to logon.

recommandation

- DigInv recommends that all pre-logon banner messages should be configured to warn against unauthorized access.

```
banner login delimiter banner-message delimiter
```

12. The BOOTP Service Was Not Disabled

Overall:LOW
Impact:LOW
Ease:Easy
Fix:Quick

observation

BOOTstrap Protocol (BOOTP) is a datagram protocol that allows compatible hosts to load their operating system over the network from a BOOTP server. Cisco routers are capable of acting as BOOTP servers for other Cisco devices and the service is enabled by default. However, BOOTP is rarely used and may represent a security risk. DigInv determined that BOOTP was not disabled. However, it is worth noting that not all Cisco devices support BOOTP.

impact

- An attacker could use the BOOTP service to download a copy of the router's IOS software.

ease

Tools are available on the Internet to access BOOTP servers.

recommandation

- DigInv recommends that, if not required, the BOOTP service be disabled. The following command can be used to disable BOOTP:

```
no ip bootp server
```

13. Clear Text HTTP Service Enabled

Overall:Medium
Impact:High
Ease:Moderate
Fix:Quick

observation

HTTP (RFC 2616) provides web-based services, such as information services, network device administration and other potentially sensitive services. HTTP provides no encryption of the connection between the client and server including any authentication and data transfer.

impact

- Due to the lack of encryption provided by the HTTP service, an attacker who is able to monitor a session would be able to view all of the authentication credentials and data passed in the session. The attacker could then attempt to gain access to the device using the authentication credentials extracted from the session and potentially gain access under the context of that user. Since HTTP is commonly used for network device administration this could gain the attacker an administrative level of access.

ease

To exploit the fact that the HTTP service does not provide any encryption, the attacker would need to be able to monitor the session between a HTTP server and web browser. In some situations the attacker may not need to perform any further action other than launching a network monitoring tool. However, in a switched network the attacker may need to perform additional actions such as an ARP attack and in a routed environment the attacker may have to compromise the network routing.Tools that are capable of both monitoring and displaying network traffic in an easy to read form can be downloaded from the Internet. There are also tools that automatically detect where authentication credentials or files are being transferred and display or save the data. Tools are also available that enable an attacker to easily perform a variety of network attacks in order to be able to monitor and intercept sessions between two network devices.

recommandation

- DigInv recommends that the HTTP service should be disabled. If remote administrative access is required then DigInv recommends that a cryptographically secure alternative, such as HTTPS, should be used instead.

```
no ip http server
```

14. TCP Small Services Enabled

Overall:INFORMATIONAL
Impact:Informational
Ease:Trivial
Fix:Quick

observation

Some devices and platforms provide a collection of simple TCP network services, which are also sometimes referred to as small services. These services provide little functionality and are rarely used and they typically include:Echo (defined in RFC 862) returns any data sent to it back to the connecting client;Discard (defined in RFC 863) ignores any data sent to it by a connecting client;Chargen (defined in RFC 864) generates printable characters which are returned to the connecting client;Daytime (defined in RFC 867) returns the current time to a connecting client.DigInv determined that the TCP small servers were enabled

impact

- Each running service increases the chances of an attacker being able to identify the device and successfully compromise it. Although not significant, some of the services may provide an attacker with simple information that could then be used as part of a targeted attack against the system.

ease

Tools such as Telnet can be used to connect to these services and are often installed by default.

recommandation

- It is generally considered good security practice to disable all unused services and not running the services will free system resources for other use. Therefore DigInv suggests that the TCP small servers should be disabled.

```
no service tcp-small-servers
```

15. No Network Filtering Rules Were Configured

Overall:INFORMATIONAL
Impact:INFORMATIONAL
Ease:N/A
Fix:Planned

observation

Network filtering can be configured to restrict access to network services from only those hosts that require the access, helping to prevent unauthorized access. When configured, network filter rules are processed sequentially and the first rule in the filter rule list which matches the network packet is applied.

impact

- Typically firewall appliances will drop network traffic if there are no network filtering rules configured. Whereas most non-firewall appliances will usually allow all network traffic if no network filtering rules have been configured. Although no network filter rules had been configured the default action was to drop the all network packets. Therefore an attacker, or malicious user, would not be able to access network services as all network traffic would be blocked.

ease

No specialist skills or tools are required by the attacker to exploit this issue.

recommandation

- DigInv recommends that network filter rules should be configured to help prevent unauthorized access to network services.DigInv recommends that: filter rules should only allow access to specific destination addresses
- filter rules should only allow access to specific destination network ports
- filter rules should only allow access from specific source addresses
- filter rules should specify a specific network protocol
- ICMP filter rules should specify a specific message type
- filter rules should always drop network packets and not reject them
- filter rules should perform a specific action and not rely on a default action.

```
access-list number [permit | deny] protocol source-address [source-port]
dest-address [dest-port] [log]
```

16. No Post Logon Banner Message

Overall:INFORMATIONAL
Impact:INFORMATIONAL
Ease:N/A
Fix:Quick

observation

Post logon banner messages are ones that are shown to users after they have authenticated and prior to being given access to the device. It is one that is shown to users when they connect to a device and prior to the user logon.

impact

- The post logon banner is useful for detailing the acceptable use policy and the change control procedures which should be followed prior to making any changes to a device's configuration. An acceptable use message detailing the change control procedures and waning against abuse of the policy could help to prevent ad- hoc changes being made to a device's configuration. Additionally, if a device does not have the facilities to configure a pre-logon banner message then the post logon banner message could be the only place where a legal warning against unauthorized access could be given.

ease

With no post logon banner configured, a user would not be given a reminder of the acceptable use and change control procedure policy details.

recommandation

- DigInv recommends that a post logon banner message is configured that details both the acceptable use policy and change control procedures. Additionally, if the device does not support a pre-logon banner message then DigInv recommends that the post logon banner message should also include a carefully worded legal warning against unauthorized access.

```
banner exec delimiter banner-message delimiter
```

17. PAD Service Enabled

Overall:INFORMATIONAL
Impact:INFORMATIONAL
Ease:N/A
Fix:Quick

observation

The PAD service enables X.25 commands and connections between PAD devices and access servers, converting the character stream data into network packets and network packets into character stream data. The PAD service is enabled by default on some devices but it is only required if support for X.25 links are necessary.

impact

- In addition to the extra overhead, running unused services increases the chances of an attacker finding a security hole or fingerprinting a device.

ease

The PAD service was enabled.

recommandation

- DigInv recommends that, if not required, the PAD service should be disabled.

```
no service pad
```

18. No Outbound TCP Connection Keep-Alives

Overall:INFORMATIONAL
Impact:INFORMATIONAL
Ease:Challenging
Fix:Quick

observation

The keep-alive messages are used to determine if a connection is active or has become orphaned and is no longer used. Depending on the result, the device can reclaim resources allocated to inbound connections that have become orphaned. Connections to a device could become orphaned if a connection becomes disrupted or if the client has not properly terminated a connection.

impact

- An attacker could attempt a DoS attack against a device by exhausting the number of possible connections. To perform this attack, the attacker could keep requesting new connections to the device and spoof the source IP addresses. This would then prevent any new legitimate connections to the device from being made as the device awaits the completion of the connection attempts that have already been initiated. This attack would prevent both users and administrators from connecting to the device.

ease

Tools can be downloaded from the Internet that are capable of opening a large number of TCP connections without correctly terminating them.

recommandation

- DigInv recommends that TCP keep alive messages should be sent to detect and drop orphaned connections from remote systems.

```
service tcp-keepalives-out
```

19. Authentication Failure Rate was not configured

Overall:INFORMATIONAL
Impact:INFORMATIONAL
Ease:Challenging
Fix:Quick

observation

Authentication for a computer system is a process allowing the system to ensure the legitimacy of the access request made by an entity (human being or another system...) in order to authorize the access of this entity to system resources (systems , networks, applications , etc.)

impact

- Allow an attacker to gain access to the device if dictionary based attack was passed succefully

ease

One method of cracking passwords, called the dictionary attack, is to use software that attempts to log in using every word in a dictionary.Tools are available in Internet

recommandation

- DigInv recommands that authentication failure rate should be configured with 3 tries or less

```
security authentication failure rate <3>
```

Interfaces Audit

20. Not All OSPF Routing Updates Were Authenticated

Overall:HIGH

observation

Impact:High
Ease:Easy
Fix:Involved

OSPF is a routing protocol that allows network devices to dynamically adapt to changes to the network topology. OSPF supports authentication using either clear-text or MD5 authentication methods. This ensures that routing updates are sent from a trusted source.

impact

- An attacker may attempt to modify the routing table of a routing device in an attempt to route network traffic through a device that they control. If an attacker is able to control a routing device they would be able to: monitor network traffic sent between network segments
- perform a man in the middle attack
- capture clear-text protocol authentication credentials
- capture encrypted authentication hashes which could be subjected to a brute-force attack
- perform a network wide DoS
- route updates could be redistributed by the device to other routing devices and possibly using other routing protocols and authentication.

ease

Tools can be downloaded from the Internet that can be used to send malicious OSPF routing updates. With no authentication configured, an attacker would not have to determine the authentication key prior to sending malicious OSPF route updates.

recommandation

- DigInv recommends that strong OSPF authentication keys should be configured for all routing updates. DigInv recommends that: OSPF authentication keys should be at least eight characters in length
- characters in the OSPF authentication key should not be repeated more than three times
- OSPF authentication keys should include both upper case and lower case characters
- OSPF authentication keys should include numbers
- OSPF authentication keys should include punctuation characters
- OSPF authentication keys should not include a device's name, make or model
- OSPF authentication keys should not be based on dictionary words.

```
ip ospf authentication message-digest
```

1. No OSPF LSA Thresholds

Overall:LOW
Impact:Medium
Ease:Moderate
Fix:Planned

observation

OSPF is a routing protocol that can be configured to dynamically update the routing table with changes to the network topology. OSPF uses LSA to communicate changes to other routers and update the routers own Link State Database (LSDB). Devices can be configured with a LSA message threshold in order to limit the number of LSA messages being processed by the device.

impact

- An attacker may be able to perform an OSPF DoS by flooding the device with LSA messages. monitor network traffic sent between network segments
- perform a man in the middle attack
- capture clear-text protocol authentication credentials
- capture encrypted authentication hashes which could be subjected to a brute-force attack
- perform a network wide DoS
- route updates could be redistributed by the device to other routing devices and possibly using other routing protocols and authentication.

ease

Tools can be downloaded from the Internet that can be used to perform a DoS by flooding the device with LSA messages.

recommandation

- DigInv recommends that the number of OSPF LSA messages accepted by the device should be limited.

```
max-lsa threshold
```

1. Connection Timeout not configured

Overall:INFORMATIONAL
Impact:Informational
Ease:Easy
Fix:Quick

observation

Connection timeouts can be configured for a number of the device services. If a timeout were configured on an administrative service, an administrator that did not correctly terminate the connection would have it automatically closed after the timeout expires. However, if a timeout is not configured, or is configured to be a long timeout, an unauthorised user may be able to gain access using the administrator's previously logged-in connection.

impact

- An attacker who was able to gain access to a connection that had not expired, would be able to continue using that connection. A connection could be a console port on the device that was not correctly terminated or a remote administrative connection.

ease

The attacker would have to gain physical access to the device to use the console port, or gain remote access to an administration machine that is attached to the port. To gain access to remote connections, an attacker would have to be able to intercept network traffic between the client and the device. The attacker would then have to take over the connection, which could be very difficult with some services. Tools are available on the Internet that would facilitate the monitoring of network connections.

recommandation

- DigInv ecommends that a timeout period of ten minutes be configured for connections to the device

```
exec-timeout time(minutes) time(seconds)
```

Vulnerabilty Audit

1. CVE-2008-3809

version:V2
score:7.1
severity:HIGH

Description

Cisco IOS 12.0 through 12.4 on Gigabit Switch Router (GSR) devices (aka 12000 Series routers) allows remote attackers to cause a denial of service (device crash) via a malformed Protocol Independent Multicast (PIM) packet.

For more details about this CVE, click this link below:
https://nvd.nist.gov/vuln/detail/CVE-2008-3809

2. CVE-2008-4128

version:V2
score:9.3
severity:HIGH

Description

Multiple cross-site request forgery (CSRF) vulnerabilities in the HTTP Administration component in Cisco IOS 12.4 on the 871 Integrated Services Router allow remote attackers to execute arbitrary commands via (1) a certain "show privilege" command to the /level/15/exec/- URI, and (2) a certain "alias exec" command to the /level/15/exec/-/configure/http URI. NOTE: some of these details are obtained from third party information.

For more details about this CVE, click this link below:
https://nvd.nist.gov/vuln/detail/CVE-2008-4128

3. CVE-2006-4950

version:V2
score:10.0
severity:HIGH

Description

Cisco IOS 12.2 through 12.4 before 20060920, as used by Cisco IAD2430, IAD2431, and IAD2432 Integrated Access Devices, the VG224 Analog Phone Gateway, and the MWR 1900 and 1941 Mobile Wireless Edge Routers, is incorrectly identified as supporting DOCSIS, which allows remote attackers to gain read-write access via a hard-coded cable-docsis community string and read or modify arbitrary SNMP variables.

For more details about this CVE, click this link below:
https://nvd.nist.gov/vuln/detail/CVE-2006-4950

4. CVE-2008-1156

version:V2
score:5.1
severity:MEDIUM

Description

Unspecified vulnerability in the Multicast Virtual Private Network (MVPN) implementation in Cisco IOS 12.0, 12.2, 12.3, and 12.4 allows remote attackers to create "extra multicast states on the core routers" via a crafted Multicast Distribution Tree (MDT) Data Join message.

For more details about this CVE, click this link below:
https://nvd.nist.gov/vuln/detail/CVE-2008-1156

5. CVE-2010-0578

version:V2
score:7.8
severity:HIGH

Description

The IKE implementation in Cisco IOS 12.2 through 12.4 on Cisco 7200 and 7301 routers with VAM2+ allows remote attackers to cause a denial of service (device reload) via a malformed IKE packet, aka Bug ID CSCtb13491.

For more details about this CVE, click this link below:
https://nvd.nist.gov/vuln/detail/CVE-2010-0578