**Knowledge Base Articles**

A compilation of KBAs that I have created

**Demonstrated Skills:**

* *Accurate Research*
* *Technical Understanding*
* *Clear and Concise Writing*
* *Organized Document Structuring*

***Dynamic Host Configuration Protocol***

*This article is designed to inform and educate the reader about Dynamic Host Configuration Protocol (DHCP), the components involved, and potential security risks to be aware of when using this protocol on a network.*

*What is DHCP? Why do we use it and what are the benefits of using DHCP?*

Dynamic Host Configuration Protocol (DHCP) is used in network management to dynamically assign the IP address and additional relevant information to network hosts. This process allows the hosts to communicate. The DHCP process is a tool used by administrators to automatically assign and manage the IP addresses for clients and devices using the network. As well, DHCP assigns and handles the [DNS](https://www.cloudflare.com/en-ca/learning/dns/what-is-a-dns-server/), [subnet masks](https://avinetworks.com/glossary/subnet-mask/) and [default gateway](https://www.lifewire.com/what-is-a-default-gateway-817771) used by the network. DHCP is beneficial because it provides reliable IP address configuration without any additional costs and reduces the overall amount of network administration required. Without DHCP, each client would need to have the IP set manually, which is time consuming and unnecessary.

*Components of Dynamic Host Configuration Protocol*

**What is a DHCP Server?**

A DHCP server is a network server that automatically provides and then assigns network functions to client devices using a network. The DHCP server handles the[IP addresses](https://en.wikipedia.org/wiki/IP_address) assigned to the clients, the domain name system (DNS), the subnet masks (which identify the host computer and network it belongs to), and the default gateway used by the network.

**What is a DHCP Client?**

A DHCP client is a device accessing a [network](https://en.wikipedia.org/wiki/Computer_network) that receives information from the [server](https://www.promax.com/blog/what-is-the-purpose-of-a-computer-server). Common examples of DHCP devices would be a computer, tablet, or mobile phone. The client receives services from the server that it connects to.

**What is a DHCP Address Pool?**

A [DHCP pool](https://techhub.hpe.com/eginfolib/networking/docs/switches/5120si/cg/5998-8491_l3-ip-svcs_cg/content/436042662.htm) is a group of internet protocol (IP) addresses that can be assigned to clients or devices on a network. The DHCP pool will assign IP addresses from a specified subnet using the gateway IP address ([GIADDR](https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-subnet-options)) and be limited to the range of addresses that are configured.

**What ARE DHCP Address Leases?**

A DHCP address lease is responsible for temporarily assigning IP addresses to network devices. These addresses are assigned from the IP address pool by the DHCP server and are only assigned to the devices for as long as they are connected to the network. A lease can be set to a [specified amount of time](https://techgenix.com/dhcp-lease-time-how-to-change-it/) before it expires. The configuration of the lease time is performed by the [network administrator](https://en.wikipedia.org/wiki/Network_administrator).

**What ARE DHCP Address Reservations?**

A DHCP address reservation is when you instruct the network to reserve a specific IP address for a device whenever that device connects to the network. An example of this would be when configuring a [network printer](https://www.linksys.com/in/support-article?articleNum=138708). This IP address is held for the designated device and is no longer available to clients and other devices using the network.

**WHAT IS A DHCP RELAY?**

A DHCP relay allows [DHCP messages](https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/dhcp/dhcp-messages.html) to be transferred between the DHCP server and clients located on different subnets. A DHCP relay converts broadcast DHCP packets into [unicast](https://en.wikipedia.org/wiki/Unicast) then forwards this information to the server.

*DHCP Security and Potential Risks*

Despite the many benefits of using DHCP, it does not come without risks. One issue is DHCP uses a limited number of IP addresses. This unfortunately could allow an unauthorized user to attempt a [denial-of-service attack](https://en.wikipedia.org/wiki/Denial-of-service_attack) by continuously requesting IP addresses from the server, tying up resources. Another issue to keep in mind is that any user receiving an IP address from the DHCP server is also receiving the [Domain Name System (DNS)](https://www.cloudflare.com/en-ca/learning/dns/what-is-a-dns-server/) and [Windows Internet Naming Service (WINS).](https://docs.microsoft.com/en-us/windows-server/networking/technologies/wins/wins-top) The user may use this to request more information they do not need to know or even worse, use this information to create an attack on the server. Administrators should also be aware that unauthorized users may attempt to set up [rogue DHCP servers](https://en.wikipedia.org/wiki/Rogue_DHCP) on the network that would provide improper IP addresses to clients as well.

*This knowledge base article was created by Jeff Guitard, a first year IT Systems Management and Security student at the NSCC Institute of Technology located in Halifax, Nova Scotia.*

**References**

DHCP and manual IP address configuration.  Retrieved from Homenet Howto website: <https://www.homenethowto.com/basics/giving-the-computer-an-ip-address/>

DHCP Lease.  Retrieved from EfficientIP website:

<https://www.efficientip.com/glossary/dhcp-lease/>

DHCP Relay Agent in Computer Network. (2018, January 17). Retrieved from GeeksforGeeks website: <https://www.geeksforgeeks.org/dhcp-relay-agent-in-computer-network/>

How does DHCP work? Retrieved from Cyber Security News website: <https://cybersecuritynews.co.uk/how-does-dhcp-work/>

How to Set Up DHCP Reservations (and Never Check an IP Address Again).  Retrieved from Lifehacker website: <https://lifehacker.com/how-to-set-up-dhcp-reservations-and-never-check-an-ip-5822605>

DHCP Security Considerations - Designing Infrastructure Windows Server 2003. Retrieved February 6, 2022, from Windows Server Brain website: <https://www.serverbrain.org/designing-infrastructure-2003/dhcp-security-considerations.html>

What is DHCP and how does it work?  Retrieved from afteracademy.com website: <https://afteracademy.com/blog/what-is-dhcp-and-how-does-it-work>

**Links used in article for additional reading**

https://www.cloudflare.com/en-ca/learning/dns/what-is-a-dns-server/

https://avinetworks.com/glossary/subnet-mask/

https://www.lifewire.com/what-is-a-default-gateway-817771

https://en.wikipedia.org/wiki/IP\_address

https://en.wikipedia.org/wiki/Computer\_network

https://www.promax.com/blog/what-is-the-purpose-of-a-computer-server

https://techhub.hpe.com/eginfolib/networking/docs/switches/5120si/cg/5998-8491\_l3-ip-svcs\_cg/content/436042662.htm

https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-subnet-options

https://techgenix.com/dhcp-lease-time-how-to-change-it/

https://en.wikipedia.org/wiki/Network\_administrator

https://en.wikipedia.org/wiki/Unicast

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/dhcp/dhcp-messages.html

https://en.wikipedia.org/wiki/Denial-of-service\_attack

https://docs.microsoft.com/en-us/windows-server/networking/technologies/wins/wins-top

https://en.wikipedia.org/wiki/Rogue\_DHCP

***Secure Socket Tunneling Protocol and VPNs***

*This article is designed to inform and educate the reader about Virtual Private Network (VPN) connections and the Secure Socket Tunneling Protocol (SSTP). Explored will be the components involved in VPNs, examples of Multi-Protocol and Single-Protocol VPNs, how SSTP works and why SSTP is so popular when using VPNs.*

*What are Virtual Private Networks and how do they work?*

A Virtual Private Network (VPN) is a tool that gives the user enhanced [privacy](https://www.winston.com/en/legal-glossary/online-privacy.html) and security. This is done by creating a [private network](https://www.sciencedirect.com/topics/computer-science/private-network) using a public internet connection. A VPN allows you to mask your [Internet Protocol (IP) address](https://en.wikipedia.org/wiki/IP_address), hiding your true IP address. This is done by allowing the network to redirect your IP through a specially configured [remote server](https://www.dnsstuff.com/windows-remote-server-administration#:~:text=Remote%20servers%20are%20designed%20to,right%20tools%20for%20the%20job.) run by the VPN host. Hiding your IP address keeps the communication between your computer and the websites you visit private. This is particularly beneficial as protection against [hackers](https://en.wikipedia.org/wiki/Hacker) seeking your personal information and [advertisers tracking](https://blog.hubspot.com/blog/tabid/6307/bid/7249/a-marketer-s-guide-to-tracking-online-campaigns.aspx) what products and services you are interested in. There are also many other [benefits](https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn) that using a VPN creates for the user and how they can browse the internet.

*Types or VPNs*

There are 3 main types of Virtual Private Networks: Remote Access VPN, Intranet based VPN and Extranet based VPN. Each of these are based on different [security protocols](https://www.igi-global.com/dictionary/security-protocol/26119#:~:text=A%20security%20protocol%20is%20essentially,to%20achieve%20a%20security%20goal.).

**Remote Access VPN**

A [remote access](https://www.techtarget.com/searchsecurity/definition/remote-access) VPN allows the user to connect to a remote server. This is how most VPN services are set up. Using a VPN service allows you to browse the internet using the VPN providers network as well as [encrypting](https://en.wikipedia.org/wiki/Encryption) your data. A side benefit of this type of VPN is that if the VPN server is in another country, it allows you to gain access to websites that may be otherwise restricted in your [region](https://en.wikipedia.org/wiki/Region). This type of VPN is best suited for personal use.

**Intranet Based VPN**

An [intranet](https://en.wikipedia.org/wiki/Intranet) based VPN is a private network created to hide private intranets and allow the users on the secured network to access each other’s resources and information. An intranet VPN would often link head office, remote offices and branch offices using dedicated connections and shared [network infrastructure](https://www.techopedia.com/definition/16955/network-infrastructure#:~:text=Network%20infrastructure%20is%20the%20hardware,and%20external%20networks%2Fthe%20internet.). This type of VPN would be best suited for large companies to ensure secure communication between departments and offices.

**Extranet Based VPN**

An [extranet](https://en.wikipedia.org/wiki/Extranet) based VPN would link customers, partners and suppliers to a company’s network using a shared infrastructure and [dedicated connections](https://www.business.org/services/internet/dedicated-internet-connection/). Extranet VPNs differ from intranet VPNs in the sense that they allow access to information and resources from users outside of the company. An example of this would be a company website that allows authorized users to access additional resources other than what is publicly shared on the company’s website.

*Single-Protocol vs Multi-Protocol VPNs*

VPN protocols connect the users device to [the VPN client](https://www.barracuda.com/glossary/vpn-client#:~:text=A%20VPN%20client%20is%20a,interact%20with%20and%20configure%20them.), [VPN tunnel](https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure) and [VPN server](https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-a-vpn-server-how-does-a-vpn-server-work/) then ultimately to the internet.

A single protocol VPN is a service that only supports one VPN protocol. An example of a single protocol VPN would be OpenVPN. OpenVPN is an open source VPN protocol that uses [Secure Socket Layer (SSL)](https://www.cloudflare.com/en-ca/learning/ssl/what-is-ssl/) to create an encrypted internet connection that requires [device authentication](https://thenextweb.com/news/the-ultimate-guide-to-selecting-a-device-authentication). The OpenVPN protocol can be configured to bypass existing [firewall](https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html) restrictions.

A multi protocol VPN offers a user multiple options for different purposes. This type of VPN could be optimized for many popular online activities such as [video streaming](https://www.techtarget.com/searchunifiedcommunications/definition/streaming-video), information exchange via messaging or [online gaming](https://en.wikipedia.org/wiki/Online_game) using different protocols. HybridVPN combines the SSL connection and a [SmartDNS](https://support.nordvpn.com/General-info/SmartDNS/1161156142/What-is-SmartDNS.htm) proxy server to provide the full security and privacy of a VPN as well.

*Secure Socket Tunneling Protocol*

**What is Secure Socket Tunneling Protocol (SSTP)?**

Secure Socket Tunneling Protocol (SSTP) was developed by [Microsoft](https://en.wikipedia.org/wiki/Microsoft) and is a type of VPN tunnel that provides a method to transport [Point-to-Point protocol (PPP](https://en.wikipedia.org/wiki/Point-to-Point_Protocol)) traffic through a [Transport Layer Security(TLS)](https://en.wikipedia.org/wiki/Transport_Layer_Security) channel. TLS provides security, encryption, and [network traffic integrity](https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Secure-Connection/getting-started-with-network-integrity-v129873021-d4152e868.html) checking. Using Transport Layer Security over [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (443 is the default port, but can be changed) will allow the SSTP to circumvent [firewalls](https://en.wikipedia.org/wiki/Firewall_(computing)) and [proxy servers](https://www.pcmag.com/encyclopedia/term/proxy-server#:~:text=A%20proxy%20server%20is%20a,on%20behalf%20of%20the%20user.) unless they are [authenticated web proxies](https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/use-authenticated-proxy-servers). SSTP is safer and more secure than the existing technologies [Layer 2 Tunneling Protocol (L2TP)](https://www.techtarget.com/searchnetworking/definition/Layer-Two-Tunneling-Protocol-L2TP#:~:text=Layer%20Two%20Tunneling%20Protocol%20(L2TP)%20is%20an%20extension%20of%20the,to%20pass%20within%20the%20tunnel.) and [Point-to-point Tunneling Protocol (PPTP)](https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol). Secure Socket Tunneling Protocol is available for [Linux](https://en.wikipedia.org/wiki/Linux), [BSD](https://en.wikipedia.org/wiki/Berkeley_Software_Distribution) and [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) operating systems.

**How Does SSTP Work?**

Secure Socket Tunneling Protocol (SSTP) creates a [secure connection](https://www.techopedia.com/definition/13266/secure-connection#:~:text=A%20secure%20connection%20is%20a,between%20two%20or%20more%20nodes.) between a VPN client and VPN server. By default, SSTP uses [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) port 443 (the same port used for [HTTPS](https://en.wikipedia.org/wiki/HTTPS) traffic). Everything (all data and traffic) that passes through the secure connection or “tunnel” is [encrypted](https://en.wikipedia.org/wiki/Encryption). SSTP servers must be authenticated when a connection is established. [Authentication](https://www.bu.edu/tech/about/security-resources/bestpractice/auth/) for SSTP clients can be optionally configured to require authentication as well.

**Why is SSTP so popular in respect to VPNs?**

There are many reasons that SSTP is such a popular VPN protocol. The most prominent reasons being that Secure Socket Tunneling Protocol offers 256 bit [Advanced Encryption Standard (AES)](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) security. SSTP is owned by Microsoft and is fully compatible and supported by Windows (the most popular choice for business networking). SSTP can also be used to circumvent firewalls and unnecessary [proxy servers](https://www.fortinet.com/resources/cyberglossary/proxy-server), resulting in improved overall user performance.

*This knowledge base article was created by Jeff Guitard, a first year IT Systems Management and Security student at the NSCC Institute of Technology located in Halifax, Nova Scotia.*

**References**

Hoffman, C. (2018, April 19). What Is a VPN, and Why Would I Need One? Retrieved from How-To Geek website: <https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/>

Kaspersky. (2020, November 3). What is a VPN and how does it work? Retrieved from www.kaspersky.com website: <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

Multi-Protocol VPN: Why You Need Different VPN Protocols in One App. (n.d.). Retrieved from www.vpnunlimited.com website: <https://www.vpnunlimited.com/help/vpn-protocols/multi-protocol-vpn>

What Is A VPN Protocol And Which One Should You Use? (2019, June 17). Retrieved March 19, 2022, from Information Security Buzz website: <https://informationsecuritybuzz.com/articles/what-is-a-vpn-protocol-and-which-one-should-you-use/>

What is SSTP VPN? Everything You Need to Know. (2022, February 7). Retrieved March 19, 2022, from PUREVPN website: <https://www.purevpn.com/what-is-vpn/protocols/sstp#:~:text=Why%20is%20SSTP%20a%20Popular>

What Is SSTP? (Your Guide to the SSTP VPN Protocol). (n.d.). Retrieved March 19, 2022, from CactusVPN website: <https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/#:~:text=SSTP%20works%20by%20establishing%20a>

**Links used in article for additional reading**

https://www.winston.com/en/legal-glossary/online-privacy.html

https://www.sciencedirect.com/topics/computer-science/private-network

https://en.wikipedia.org/wiki/IP\_address

https://www.dnsstuff.com/windows-remote-server-administration#:~:text=Remote%20servers%20are%20designed%20to,right%20tools%20for%20the%20job.

https://en.wikipedia.org/wiki/Hacker

https://blog.hubspot.com/blog/tabid/6307/bid/7249/a-marketer-s-guide-to-tracking-online-campaigns.aspx

https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

https://www.techtarget.com/searchnetworking/definition/Layer-Two-Tunneling-Protocol-L2TP#:~:text=Layer%20Two%20Tunneling%20Protocol%20(L2TP)%20is%20an%20extension%20of%20the,to%20pass%20within%20the%20tunnel.

https://www.igi-global.com/dictionary/security-protocol/26119#:~:text=A%20security%20protocol%20is%20essentially,to%20achieve%20a%20security%20goal.

https://en.wikipedia.org/wiki/Encryption

https://en.wikipedia.org/wiki/Region

https://en.wikipedia.org/wiki/Intranet

https://en.wikipedia.org/wiki/Microsoft

https://en.wikipedia.org/wiki/Intranet

https://en.wikipedia.org/wiki/Point-to-Point\_Tunneling\_Protocol

https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

https://en.wikipedia.org/wiki/Wide\_area\_network

https://www.barracuda.com/glossary/vpn-client#:~:text=A%20VPN%20client%20is%20a,interact%20with%20and%20configure%20them.

https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure

https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-a-vpn-server-how-does-a-vpn-server-work/

https://www.cloudflare.com/en-ca/learning/ssl/what-is-ssl/

https://thenextweb.com/news/the-ultimate-guide-to-selecting-a-device-authentication

https://en.wikipedia.org/wiki/Transport\_Layer\_Security

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Secure-Connection/getting-started-with-network-integrity-v129873021-d4152e868.html

https://en.wikipedia.org/wiki/Transmission\_Control\_Protocol

https://www.pcmag.com/encyclopedia/term/proxy-server#:~:text=A%20proxy%20server%20is%20a,on%20behalf%20of%20the%20user.

https://en.wikipedia.org/wiki/Linux

https://en.wikipedia.org/wiki/Berkeley\_Software\_Distribution

https://en.wikipedia.org/wiki/Microsoft\_Windows

https://www.techopedia.com/definition/13266/secure-connection#:~:text=A%20secure%20connection%20is%20a,between%20two%20or%20more%20nodes.

https://en.wikipedia.org/wiki/Transmission\_Control\_Protocol

https://en.wikipedia.org/wiki/HTTPS

https://en.wikipedia.org/wiki/Encryption

https://www.bu.edu/tech/about/security-resources/bestpractice/auth/

https://en.wikipedia.org/wiki/Extranet

https://www.business.org/services/internet/dedicated-internet-connection/

https://en.wikipedia.org/wiki/Online\_game

https://www.fortinet.com/resources/cyberglossary/proxy-server

Introduction

***CVE-2022-37968***

This document contains information aboutCVE-2022-37968, the [Azure Arc](https://learn.microsoft.com/en-us/azure/azure-arc/overview)-enabled [Kubernetes](https://kubernetes.io/) cluster connect [Elevation Of Privilege](https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/elevation-of-privilege) security vulnerability. The document will include details of the CVE-2022-37968vulnerability, the risk of attack severity, known fixes to date and how to protect yourself in the future. Links to additional resources on the Azure Arc-enabled Kubernetes cluster connect Elevation of Privilege vulnerability will be provided as well.

Author Information

*The author of this article, Jeff Guitard, is a second year IT Systems Management and Security student at the NSCC Institute of Technology located in Halifax, Nova Scotia.*

CVE-2022-37968 is a [network vulnerability](https://www.itsasap.com/blog/what-is-security-vulnerability#:~:text=Network%20Vulnerabilities%C2%A0,configured%20firewalls.)that allows an unauthenticated user to elevate their privilege. This vulnerability can be exploited by attackers using the internet to gain access.

 e Arc-enabled Kubernetes cluster connect Elevation of Privilege vulnerability

The official CVE-2022-37968 security vulnerability advisory was released by Microsoft on October 11, 2022. This vulnerability could allow an unauthenticated user to elevate their privileges to cluster administrator and gain administrative control over the Kubernetes cluster in an Azure Arc environment. Azure Arc allows clients to connect to on-site infrastructure such as servers and the Kubernetes system used for automating deployment and management of containerized applications. The products affected are [Azure Stack Edge](https://azure.microsoft.com/en-us/products/azure-stack/edge/#benefits:~:text=Azure%20Stack%20Edge%20acts,to%20Azure%20and%20back.) and Azure Arc. If an attacker is aware of the external [DNS](https://www.fortinet.com/resources/cyberglossary/what-is-dns) endpoint for an Azure Arc cluster with Kubernetes enabled, they can exploit this vulnerability from the internet.

Risk of Attack

This vulnerability is rated with the highest severity of **10/10 (HIGH)** on the [CVSS scale](https://www.balbix.com/insights/understanding-cvss-scores/).

Possible Fixes

[Automatic upgrade](https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-automatic-upgrade) is enabled by default for Azure Arc customers, but if this feature is disabled, manual update is required. Microsoft recommends that customers using Azure Arc-enabled Kubernetes clusters upgrade to agent versions 1.5.8 and above, 1.6.19 and above, 1.7.18 and above, or 1.8.11 as required by their system to be properly protected from this vulnerability. Customers using Azure Stack Edge must update to the 2209 release (software version 2.2.2088.5593).

How to Protect Yourself

To protect yourself in the future from this and any other potential Azure-Arc related vulnerabilities as they arise, the automatic upgrade feature should be enabled to allow all application updates to be applied as soon as they are released.

Additional Resources

**Additional Reading:**

[CVE-2022-37968 - Security Update Guide - Microsoft - Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37968)

[CVE-2022-37968 - OpenCVE](https://www.opencve.io/cve/CVE-2022-37968#:~:text=Vulnerabilities%20%28CVE%29%20CVE-2022-37968%20A%20zure%20Arc-enabled,Kubernetes%20cluster%20Connect%20Elevation%20of%20Privilege%20Vulnerability.)

References

Azure Stack Edge | Microsoft Azure. Retrieved from azure.microsoft.com website: <https://azure.microsoft.com/en-us/products/azure-stack/edge/>

Balbix. What are CVSS Scores. Retrieved from Balbix website: <https://www.balbix.com/insights/understanding-cvss-scores/>

Azure AD Connect: Automatic upgrade. Retrieved from learn.microsoft.com website: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-automatic-upgrade>

What is a Security Vulnerability? (Definition, Types, and Remediation). Retrieved from www.itsasap.com website: <https://www.itsasap.com/blog/what-is-security-vulnerability#:~:text=Network%20Vulnerabilities%C2%A0>

Elevation of Privilege - WCF. Retrieved from learn.microsoft.com website: <https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/elevation-of-privilege>

Kubernetes. Production-Grade Container Orchestration. Retrieved from Kubernetes.io website: <https://kubernetes.io/>

Fortinet. What Is DNS? Definition & How DNS Works. Retrieved from Fortinet website: <https://www.fortinet.com/resources/cyberglossary/what-is-dns>

Security Update Guide - Microsoft Security Response Center. Retrieved from msrc.microsoft.com website: <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37968>

What is Azure—Microsoft Cloud Services | Microsoft Azure. Retrieved from azure.microsoft.com website: <https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-azure/>

***CVE-2022-44704***

This document contains information aboutCVE-2022-44704, the [Microsoft Windows System Monitor](https://en.wikipedia.org/wiki/Performance_Monitor) (Sysmon) [Elevation Of Privilege](https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/elevation-of-privilege) security vulnerability. The document will include details of the CVE-2022-44704 vulnerability, the [risk of attack severity](https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/#:~:text=including%20the%20vulnerability.-,What%20is%20the%20Common%20Vulnerability%20Scoring%20System%20(CVSS),that%20do%20not%20use%20CVSS%2C%20you%20can%20use%20the%20NVD%20calculator.,-Severity%20of%20top), known fixes to date and how to protect yourself in the future. Links to additional resources on the Microsoft Windows System Monitor Elevation of Privilege Vulnerability will be provided as well.

Author Information

*The author of this article, Jeff Guitard, is a second year IT Systems Management and Security student at the NSCC Institute of Technology located in Halifax, Nova Scotia.*

Vulnerability Type

CVE-2022-44704 is a [system vulnerability](https://www.itsasap.com/blog/what-is-security-vulnerability#:~:text=Network%20Vulnerabilities%C2%A0,configured%20firewalls.)that could allow a [locally authenticated](https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview) attacker to manipulate information on Windows System Monitor (Sysmon) to gain [escalation](https://delinea.com/blog/windows-privilege-escalation#:~:text=Vertical%20privilege%20escalation%2C%20sometimes%20referred%20to%20as%20privilege,the%20compromised%20account%20to%20the%20local%20administrator%20group.) from a local user to a system administrator.

Microsoft Windows System Monitor Elevation of Privilege vulnerability

The official CVE-2022-44704 security vulnerability advisory was released by Microsoft on December 13, 2022. This vulnerability could allow a locally authenticated attacker to manipulate information on Windows System Monitor (Sysmon) to gain escalation from a local user to a system administrator.

Windows System Monitor is a built in Windows tool that allows the user to analyze [system resources](https://computer.howstuffworks.com/question466.htm). When Windows System Monitor is accessed by administrators, additional [performance counters](https://www.nextofwindows.com/10-important-windows-performance-counters-you-should-know-of) can be accessed that provide data that is restricted to non-administrative users.

Windows 7, Windows 8.1, Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, and Windows Server 2019 are all at risk to this vulnerability.

Risk of Attack

This vulnerability is rated with a **7.8/10 (HIGH)** on the [CVSS scale](https://www.balbix.com/insights/understanding-cvss-scores/).

 le Fixes

To patch this system vulnerability, Windows System Monitor must be updated to at least [build number 14.13](https://download.sysinternals.com/files/Sysmon.zip). As of January 25, 2023, [Sysmon v14.14](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon) is available as well as the most recent version.

This security update to the Sysmon.exe file was released on December 13, 2022, the same day that the vulnerability advisory was released.

How to Protect Yourself

To protect yourself in the future from this and other Windows Operating System vulnerabilities, the [Windows Update](https://en.wikipedia.org/wiki/Windows_Update) feature should be enabled to allow system updates to be applied as they are released.

Additional Resources

**Additional Reading:**

[CVE-2022-44704 - Security Update Guide - Microsoft - Microsoft Windows System Monitor (Sysmon) Elevation of Privilege Vulnerability](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44704)

[National Vulnerability Database - CVE-2022-44704 (nist.gov)](https://nvd.nist.gov/vuln/detail/CVE-2022-44704)

[What are CVSS Scores](https://www.balbix.com/insights/understanding-cvss-scores/)

[How to use Performance Monitor on Windows 10 | Windows Central](https://www.windowscentral.com/how-use-performance-monitor-windows-10)

References

NVD - CVE-2022-44704. Retrieved from nvd.nist.gov website: <https://nvd.nist.gov/vuln/detail/CVE-2022-44704>

Security Update Guide - Microsoft Security Response Center. Retrieved from msrc.microsoft.com website: <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-44704>

What are CVSS Scores. Retrieved from Balbix website: <https://www.balbix.com/insights/understanding-cvss-scores/>

December 2022 Patch Tuesday: Get Latest Security Updates from Microsoft and More. Retrieved from The Hacker News website: <https://thehackernews.com/2022/12/december-2022-patch-tuesday-get-latest.html>

Additional links used for reader comprehension

<https://en.wikipedia.org/wiki/Performance_Monitor>

<https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/elevation-of-privilege>

<https://www.imperva.com/learn/application-security/cve-cvss-vulnerability>

<https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview>

<https://delinea.com/blog/windows-privilege-escalation>

<https://computer.howstuffworks.com/question466.htm>

<https://www.nextofwindows.com/10-important-windows-performance-counters-you-should-know-of>

<https://download.sysinternals.com/files/Sysmon.zip>

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

<https://en.wikipedia.org/wiki/Windows_Update>