

Windows System Security Vulnerabilities

William Saxon

3/5/2024

The first thing that needs to be understood about vulnerabilities is what are they? A vulnerability is some kind of weakness in a system that can be exploited. There are a lot of different ways that something could be a weakness. One weakness is not locking the door. An open door is a vulnerability because anyone can come in. A bad lock doesn't do much good if it can easily be broken. So even if the door is locked than that doesn't mean no one can open it. Should people even be allowed to get to the door? If there is an important room you would want to keep people away from it. In this case the vulnerability is letting people close enough to mess with the door. What does that have to do with cybersecurity? After all getting into a room isn't getting into a computer is it? Well, it could be. Someone could just walk into a room and leave a virus or copy the data on the computer in there. That is why you need to look at vulnerabilities in more than one way. If you are only trying to protect the system from cyberattacks then you might miss something obvious like an open door. Computers also have an open door you could say. That open door are network ports. Computers use network ports to send some types of data over the network. Port 80 and 443 are used for websites with HTTP and HTTPS (Brown, 2020). Not every port is useful or good. An open port that doesn't need to be open can be a vulnerability. A hacker can use an unsecure port to get into a system. When there is a chance that a vulnerability will be used it is called a threat. A way to get rid of the threat or greatly reduce it is to close the unneeded or unsecure ports. If port 22 is known to have a common exploit, then closing that port will remove the vulnerability of having it open.

It should be no surprise that there are a lot of vulnerabilities in a Windows system. A Windows Operating System is huge and very complex. There are so many parts that there's bound to be some holes between them. It's not possible to test every part of something that massive.

Windows System Security Vulnerabilities

Even if you do test something there might be something that you missed. Maybe there's a line of code that isn't working how you think it should be working. One small line of code could crash the whole system or let a hacker in. So what is Microsoft doing about all these vulnerabilities? One of the ways is to collect bug reports. You can submit a bug and vulnerability to Microsoft to review. There's a bug bounty so if your vulnerability is bad enough, they might pay you for finding it. All the steps are from Microsoft Security Response Center (MSRC)'s website. The first step once Microsoft gets the bug report is to check if it's worth looking into. Maybe it is already being worked on or it's not actually a security vulnerability. After reviewing it and deciding that it is something worth looking into Microsoft will try to replicate the vulnerability. There are two reasons for this. The first is that your bug might be a one-off thing. A strange oddity that probably won't happen again. The second reason is that they need to understand how it works. If they can't replicate it, then they might not be able to figure out the root cause of the problem. The next step is to send the results to the right team and start working on fixing the bug. You will get progress reports on the status of the fix. If someone else also submitted the same bug or is having a similar problem related to the fix, both of you will be informed about the progress. Once the bug is fixed there might be a delay before you can get the patch. "Cases in the 'Release' state are in preparation for release. Sometimes this means they are awaiting official publication as part of our monthly Patch Tuesday release, or other service update" (Msrc, 2023). Finally, once the patch gets released, your case will be marked as complete.

If you are looking for a vulnerability where do you go? If you did a vulnerability scan using some type of scanning program and a list of codes pop up, how do you know what they mean? Which ones actually matter? That's where the Common Vulnerabilities and Exposures (CVE) and

the National Vulnerability Database (NVD) are used. Below is an example of a listing from the NVD.

CVE-2022-42973 Detail

Description

A CWE-798: Use of Hard-coded Credentials vulnerability exists that could cause local privilege escalation when local attacker connects to the database. Affected Products: APC Easy UPS Online Monitoring Software (Windows 7, 10, 11 & Windows Server 2016, 2019, 2022 - Versions prior to V2.5-GA), APC Easy UPS Online Monitoring Software (Windows 11, Windows Server 2019, 2022 - Versions prior to V2.5-GA-01-22261), Schneider Electric Easy UPS Online Monitoring Software (Windows 7, 10, 11 & Windows Server 2016, 2019, 2022 - Versions prior to V2.5-GS), Schneider Electric Easy UPS Online Monitoring Software (Windows 11, Windows Server 2019, 2022 - Versions prior to V2.5-GS-01-22261)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **CNA:** Schneider Electric SE

Base Score: 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is displayed, but the Acceptance Level icon for the CNA is given a checkmark to signify NVD concurrence.

NVD <https://nvd.nist.gov/vuln/detail/CVE-2022-42973>

The next is the same vulnerability from CVE.

CVE ID	
CVE-2022-42973	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description A CWE-798: Use of Hard-coded Credentials vulnerability exists that could cause local privilege escalation when local attacker connects to the database. Affected Products: APC Easy UPS Online Monitoring Software (Windows 7, 10, 11 & Windows Server 2016, 2019, 2022 - Versions prior to V2.5-GA), APC Easy UPS Online Monitoring Software (Windows 11, Windows Server 2019, 2022 - Versions prior to V2.5-GA-01-22261), Schneider Electric Easy UPS Online Monitoring Software (Windows 7, 10, 11 & Windows Server 2016, 2019, 2022 - Versions prior to V2.5-GS), Schneider Electric Easy UPS Online Monitoring Software (Windows 11, Windows Server 2019, 2022 - Versions prior to V2.5-GS-01-22261)	
References Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete. - MISC:https://download.schneider-electric.com/files?p_Doc_SEVD-2022-347-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-347-01_Easy_UPS_Online_Monitoring_Software_Security_Notification.pdf - URL:https://download.schneider-electric.com/files?p_Doc_SEVD-2022-347-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-347-01_Easy_UPS_Online_Monitoring_Software_Security_Notification.pdf	
Assigning CNA Schneider Electric SE	
Date Record Created 20221017	
Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.	

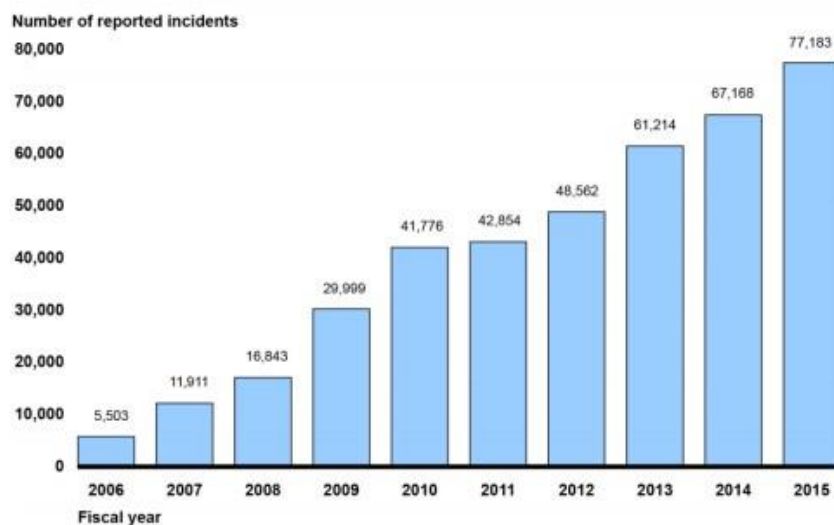
CVE <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42973>

The NVD entry is more detailed and has a risk rating. The rating goes from 0 no risk to 10.0 highest possible risk. The NVD and the CVE records are synced so what's the point of CVE if it's less detailed than NVD? According to "CVEs and the NVD Process" from nvd.nist.gov, NVD take the entries from CVE and studies them. That is where the rating, tags and extra details come from. Depending on how long it takes to look over the vulnerability, CVE might have it a bit before it gets to the NVD site.

What is the Government doing about these vulnerabilities? Not as in protections on Government systems but more in general? There are some laws to help protect people and systems. One law is the Health Insurance Portability and Accountability (HIPAA). There are four major parts. The first is “standards for electronic health information transactions” (*Health Insurance...of 1996*). These standards are the ways that security should be handled. There’re also more standards than just security. Others include enrollment, eligibility, and payment methods. The second major part of HIPAA is “Mandate on providers and health plans, and timetable” (*Health Insurance...of 1996*). When there are new standards or updates to previously existing ones, health related providers must comply within two years. If two years have passed and the new standards are not in circulation then there will big penalties and fines. The third part of HIPAA is Privacy. Congress is required to be given privacy recommendations by the Secretary every 12 months. Congress will decide what privacy legislation will be put into law and HIPAA. The last major part of HIPAA is the “Pre-emption of State Law” (*Health Insurance...of 1996*). HIPAA supersedes state laws. So if there is a state law that says one thing about security and HIPAA says something else, then when it is health related you have to follow HIPAA. The exception to this is when a state privacy law is stricter than HIPAA, the state law will be followed. Another law is the Homeland Security Act of 2002. One of the goals is “one DHS, one enterprise, a shared vision, with integrated results-based operations” (*The Department's Five... 2018*). What that means is to combine a bunch of departments to work together as one. If you have a lot of security departments that are just working on their own thing in their field then that could be a problem. If the different departments work together and share the results it could help find security holes that could have been missed otherwise.

How bad are cyberattacks getting? A lot of simple attacks have been fixed. Older attacks don't work anymore. Once the patch is out the attack can't be done anymore. As long as the system has been updated you are good to go. There is always another new type of attack waiting to pop up. Really complicated systems like Windows has so many moving parts that you could still be finding holes 10 years later. Another problem with a lot of software is all the updates. A lot of updates have patches to fix security issues, but they always add new features. With new features also brings the chance for new bugs and exploits to show up. Sometimes you have no idea how a new feature can open a hole until someone uses it to break in. Every time a patch goes out hacker will try to find more ways to break the system.

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-501

<https://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006>

This graph shows that how much cyberattacks have been increasing from 2006 to 2015. The number goes up every year. “In 2022, 800,944 cyber-crimes were reported in the US” (USAFacts, 2023). In seven years cyberattacks has increased over ten times. That number will just keep going up. One reason why the number is increasing so much is because there are more computers. The

Windows System Security Vulnerabilities

more computers there are the more that can be hit with an attack. Some attacks are targeted to certain groups hoping for a high payout. Other attacks try to be as widespread as possible. The bigger the net the more fish you can catch. Each attack might be lower than one big payout, but you have a lot more chances to get something.

Windows has a few security features built in. Patches only go so far. You might be able to make one vulnerability go away by closing the hole but that doesn't work on everything. Some viruses and worms work with Windows features to cause problems. The Windows features might be doing what they are supposed to do but in the wrong hands. That is where Windows Security comes in. "Windows Security continually scans for malware (malicious software), viruses, and security threats" (support.microsoft.com). Viruses has a signature. A bit code that acts like a fingerprint. That part of a virus is the main part of the code. How anti-malware works is that it looks for those signatures and blocks them. The anti-malware in Windows Security is called Microsoft Defender Antivirus. It used to be called Windows Defender Security Center (support.microsoft.com). There is a problem with all antivirus software. They need to have the virus's signature. It's easy for virus makers to change the code a bit to give off a different signature. Microsoft Defender Antivirus needs to be kept up to date. Windows should automatically download the updates in the background. These updates usually don't require the system to be restarted like other Windows updates. You can also go to Windows Update in the settings to force the updates to download. Another part of Windows Security is the Windows Defender Firewall. A firewall can allow or block types of network traffic. One way to use a firewall is to block a known bad network port. Some ports have big security vulnerabilities. Windows Hello uses facial

recognition to unlock the device. It has the convince of not needing to type a password. It's built into a lot of laptops. A fingerprint reader might be used instead.

In conclusion, vulnerabilities are important to look at. They are everywhere. Inside the computer with bugs and security holes like a bad network port. Also outside the computer from leaving the server room open. Windows is complicated with so many moving parts it's amazing that it even works to begin with. There's bound to be some holes that nobody thought to test. That is where the bug report comes into play. Submitting a report to Microsoft can help them get rid of previously unknown issues. Using a site like NVD helps in finding specific vulnerabilities. You can find the risk rating and maybe some ways to keep the vulnerability from happening. Government laws like HIPAA are very important. Some companies might want to cheap out on security to save some money. Health information is very dangerous to get in the wrong hands. HIPAA sets a minimum level of security that must be followed. There are more laws like HIPAA and some places need to keep track of all the rules under every category they fall into. The number of vulnerabilities and attacks just go up every year. It's not slowing down. More and more computers are being used. It's not one computer for each house anymore. People have phones, laptops, work computers, iPads and that just for one person. A normal house could have 10 computers. That's not even counting Smart Home devices. With all these systems no wonder attacks keep going up. Windows Security does its best to protect the system with added defense but it isn't perfect. Cybersecurity isn't a set once and it's good. The processes constantly need to be updated. There will always be another attack that slips through the defense. Managing vulnerabilities to fight back as much as possible is key to protect the systems.

Work Cited

- Bhattacharyya, S. (2016, June 22). *Cyberattacks against the US Government up 1,300% since 2006*. The Fiscal Times. <https://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006>
- Brown, T. (2020, December 30). *What is an SSL port? A technical guide for HTTPS*. GoDaddy Blog. <https://www.godaddy.com/resources/skills/whats-an-ssl-port-a-technical-guide-for-https>
- CVE-2022-42973 Detail*. NVD. (2023, August 2). <https://nvd.nist.gov/vuln/detail/CVE-2022-42973>
- CVE-2022-42973*. CVE. (n.d.). <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42973>
- CVEs and the NVD Process*. NVD. (n.d.). <https://nvd.nist.gov/general/cve-process>
- The Department's Five responsibilities: Homeland security*. U.S. Department of Homeland Security. (2018, September 20). <https://www.dhs.gov/blog/2009/06/08/department%E2%80%99s-five-responsibilities>
- Health Insurance Portability and accountability act of 1996*. ASPE. (1996, August 20). <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>
- Msrc. (2023, July 14). *Microsoft*. MSRC Blog | Microsoft Security Response Center. <https://msrc.microsoft.com/blog/2023/07/what-to-expect-when-reporting-vulnerabilities-to-microsoft/>
- Stay protected with Windows Security*. Microsoft Support. (n.d.). <https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963>
- USAFacts. (2023, November 20). *How many cyber-attacks occur in the US?* <https://usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us/>