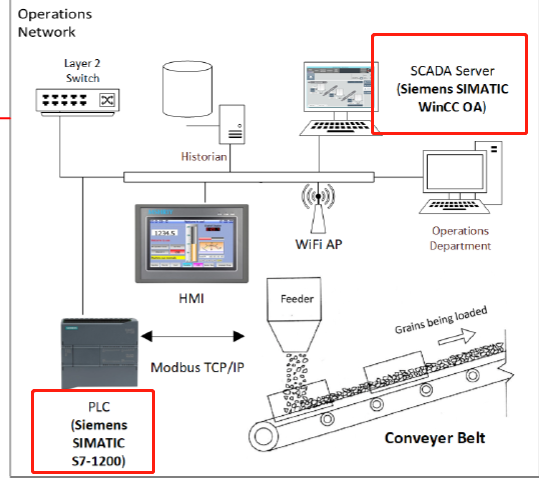
1. Introduction (Name Student ID) 30-40s
2. Aim and Goal 20S

Connect OP and Enterprise networks

At this stage the port authority is only interested in connecting their conveyor belt system to their Enterprise Network.

1. Provide an overview of the scope of your investigation. For this task, you should provide details of the port’s operations, IT and OT infrastructure that are included in your investigation. (1-2)
2. Identify a vulnerable device in the Operations Network



Since their OT infrastructure has been very stable, the last time the OT components were patched and updated were in 2013

Siemens SIMATIC S7-1200

|  |  |
| --- | --- |
| [CVE-2016-2846](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2846) | Siemens SIMATIC S7-1200 CPU devices before 4.0 allow remote attackers to bypass a "user program block" protection mechanism via unspecified vectors. 6.4 |
| [CVE-2015-5698](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5698) | Cross-site request forgery (CSRF) vulnerability in the web server on Siemens SIMATIC S7-1200 CPU devices with firmware before 4.1.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors. 7.5 |
| [CVE-2015-1048](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1048) | Open redirect vulnerability in the integrated web server on Siemens SIMATIC S7-1200 CPU devices with firmware before 4.1 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. 4.3 |
| [CVE-2014-2909](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2909) | CRLF injection vulnerability in the integrated web server on Siemens SIMATIC S7-1200 CPU devices 2.x and 3.x allows remote attackers to inject arbitrary HTTP headers via unspecified vectors. 5.8 |
| [CVE-2014-2908](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2908) | Cross-site scripting (XSS) vulnerability in the integrated web server on Siemens SIMATIC S7-1200 CPU devices 2.x and 3.x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. 4.3 |
| [CVE-2014-2258](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2258) | Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted HTTPS packets, a different vulnerability than CVE-2014-2259. 7.8 |
| [CVE-2014-2256](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2256) | Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted ISO-TSAP packets, a different vulnerability than CVE-2014-2257. 7.8 |
| [CVE-2014-2254](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2254) | Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted HTTP packets, a different vulnerability than CVE-2014-2255. 7.8 |
| [CVE-2014-2252](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2252) | Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted PROFINET packets, a different vulnerability than CVE-2014-2253. 6.1 |
| [CVE-2014-2250](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2250) | The random-number generator on Siemens SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 does not have sufficient entropy, which makes it easier for remote attackers to defeat cryptographic protection mechanisms and hijack sessions via unspecified vectors, a different vulnerability than CVE-2014-2251. 8.3 |
| [CVE-2014-2249](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2249) | Cross-site request forgery (CSRF) vulnerability on Siemens SIMATIC S7-1500 CPU PLC devices with firmware before 1.5.0 and SIMATIC S7-1200 CPU PLC devices with firmware before 4.0 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors. 5.8 |

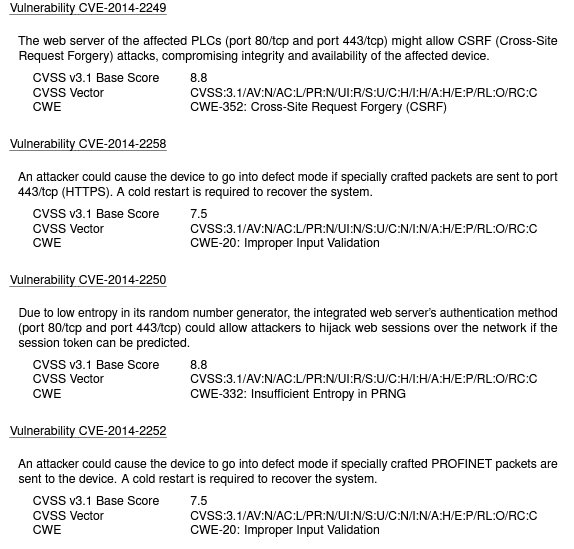
SIEMENS SIMATIC WinCC OA

|  |  |
| --- | --- |
| [CVE-2018-4847](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4847) | A vulnerability has been identified in SIMATIC WinCC OA Operator iOS App (All versions < V1.4). Insufficient protection of sensitive information (e.g. session key for accessing server) in Siemens WinCC OA Operator iOS app could allow an attacker with physical access to the mobile device to read unencrypted data from the app's directory. Siemens provides mitigations to resolve the security issue. 2.1 |
| [CVE-2018-4844](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4844) | A vulnerability has been identified in SIMATIC WinCC OA UI for Android (All versions < V3.15.10), SIMATIC WinCC OA UI for iOS (All versions < V3.15.10). Insufficient limitation of CONTROL script capabilities could allow read and write access from one HMI project cache folder to other HMI project cache folders within the app's sandbox on the same mobile device. This includes HMI project cache folders of other configured WinCC OA servers. The security vulnerability could be exploited by an attacker who tricks an app user to connect to an attacker-controlled WinCC OA server. Successful exploitation requires user interaction and read/write access to the app's folder on a mobile device. The vulnerability could allow reading data from and writing data to the app's folder. At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue. 3.8 |
| [CVE-2014-1699](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1699) | Siemens SIMATIC WinCC OA before 3.12 P002 January allows remote attackers to cause a denial of service (monitoring-service outage) via malformed HTTP requests to port 4999. 5.0 |
| [CVE-2014-1698](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1698) | Directory traversal vulnerability in Siemens SIMATIC WinCC OA before 3.12 P002 January allows remote attackers to read arbitrary files via crafted packets to TCP port 4999. 5.0 |
| [CVE-2014-1697](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1697) | The integrated web server in Siemens SIMATIC WinCC OA before 3.12 P002 January allows remote attackers to execute arbitrary code via crafted packets to TCP port 4999. 7.5 |
| [CVE-2014-1696](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1696) | Siemens SIMATIC WinCC OA before 3.12 P002 January uses a weak hash algorithm for passwords, which makes it easier for remote attackers to obtain access via a brute-force attack. 5.0 |

<https://www.cvedetails.com/cve/CVE-2014-2250>

<https://cert-portal.siemens.com/productcert/pdf/ssa-654382.pdf>

https://www.cisa.gov/news-events/ics-advisories/icsa-14-079-02



Vulnerability CVE-2014-2250, also known as the "Siemens SIMATIC S7-1200 PLC Password Hash Retrieval" vulnerability, is a security flaw that affects Siemens SIMATIC S7-1200 programmable logic controllers (PLCs).

The vulnerability allows an attacker to retrieve the password hash of an administrative user on the affected PLC without authentication. This can give the attacker access to the administrative interface of the PLC and the ability to modify the configuration, programs, and data stored on the device.

The proof of concept for this vulnerability involved sending a specially crafted HTTP request to the administrative interface of the PLC. This request contained a specific string of characters that triggered the vulnerability and allowed the attacker to retrieve the password hash.

The impact of this vulnerability is significant, as it can allow attackers to gain unauthorized access to critical industrial control systems (ICS) that are used in a wide range of industries, including manufacturing, energy, and transportation. This access could allow attackers to disrupt operations, cause physical damage, and even harm human lives.

To mitigate this vulnerability, Siemens released a security update that addresses the issue by requiring authentication for password hash retrieval. In addition, Siemens recommends that affected users implement security measures such as network segmentation, access control, and intrusion detection systems to further protect their systems.

In conclusion, vulnerability CVE-2014-2250 is a critical security flaw that affects Siemens SIMATIC S7-1200 PLCs. The vulnerability allows attackers to retrieve the password hash of an administrative user without authentication, potentially giving them access to critical ICS systems. Siemens has released a security update to address the vulnerability, and affected users should implement additional security measures to protect their systems.

1. Perform threat modelling based on the vulnerable device that you have identified in the previous task. Put yourself in the attackers’ position and create an attack tree outlining possible means to exploit the vulnerability to disrupt the ports’ operations. Describe the attack tree in detail.

* Description of the subject to be modeled
* Assumptions that can be checked or challenged in the future as the threat landscape changes
* Potential threats to the system
* Actions that can be taken to mitigate each threat
* A way of validating the model and threats, and verification of success of actions taken

Attack detail:

1. Attack Wi-Fi access point (2010-2013 WEP/WPA/WPA2(Rare)， WPA3 initial at 2018)
2. Accessing operations network
3. Initial attack on affected device
4. Gain access to target device, belt

3-4 mins

1. Identify two other (not including the above vulnerable device you have already identified) security concerns based on the information provided. You should also elaborate the potential consequences of these security concerns.

|  |  |
| --- | --- |
| [CVE-2014-1697](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1697) | The integrated web server in Siemens SIMATIC WinCC OA before 3.12 P002 January allows remote attackers to execute arbitrary code via crafted packets to TCP port 4999. 7.5 |

This vulnerability allows an attacker to execute arbitrary code on the affected system by sending a specially crafted HTTP request to the vulnerable web server. The vulnerability is caused by a buffer overflow in the web server's handling of certain HTTP requests, which can be exploited by an attacker to execute arbitrary code with elevated privileges.

The proof of concept for this vulnerability involves crafting a malicious HTTP request that triggers the buffer overflow in the vulnerable web server. Once the request is processed by the web server, the attacker can execute arbitrary code on the affected system.

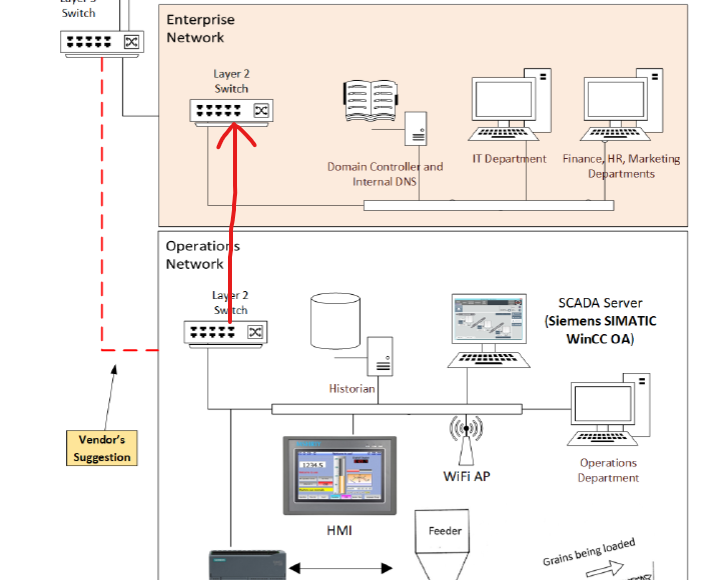
The impact of this vulnerability is significant, as it can allow an attacker to take complete control of the affected system. This can include stealing sensitive data, installing malware, and even using the system as a launching pad for further attacks against other systems on the network.

WIFI AP

PCs because of virus Similar to Stuxnet

1. Do you agree with the vendor’s suggestion? Elaborate and justify your answer. If you do not agree, suggest an alternative approach.

No.



* 1. Switch 2 -> L2
  2. Setting routing rules on Enterprise network’s L2 switch
  3. Remove Wifi AP
  4. PC disable USB
  5. Patch all devices to latest firmware, update all OS and software.

Test word.(Test, 2020)

# References

Test. (2020). *CVE-1233-3333.* 112.