Vulnerability

Vulnerability

What are vulnerabilities?

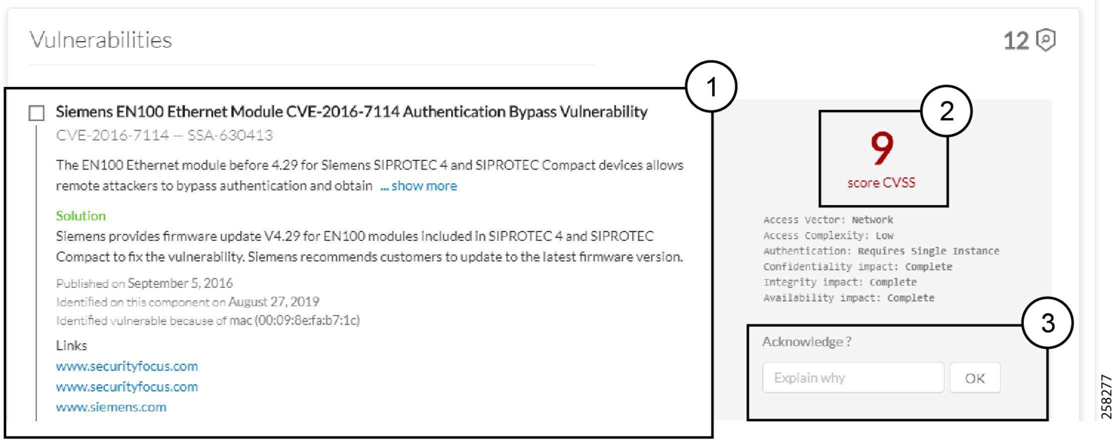
Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

Vulnerabilities are detected in Cisco Cyber Vision thanks to rules stored in the Knowledge DB. These rules are sourced from several CERTs (Computer Emergency Response Team), manufacturers and partner manufacturers (Schneider, Siemens...). Technically, vulnerabilities are generated from the correlation of the Knowledge DB rules and normalized device and component properties. A vulnerability is detected when a device or a component matches a Knowledge DB rule.

Important It is important to update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities. To do so, refer to the corresponding documentation.

What are vulnerabilities used for?

Example of a Siemens component's vulnerability visible on its technical sheet under the Security tab:



□ Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability

CVE-2016-7114 — SSA-630413

The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain ... show more

Solution

Siemens provides firmware update V4.29 for EN100 modules included in SIPROTEC 4 and SIPROTEC Compact to fix the vulnerability. Siemens recommends customers to update to the latest firmware version.

Published on September 5, 2016
Identified on this component on August 27, 2019
Identified vulnerable because of mac (00:09:8e:fa:b7:1c)

Links
www.securityfocus.com
www.securityfocus.com
www.siemens.com

9
score CVSS

```
Access Vector: Network
Access Complexity: Low
Authentication: Requires Single Instance
Confidentiality impact: Complete
Integrity impact: Complete
Availability impact: Complete
```

Acknowledge ?

Information displayed about vulnerabilities **(1)** includes the vulnerability type and reference, possible consequences and solutions or actions to take on the network. Most of the time though, it is enough to upgrade the device firmware. Some links to the manufacturer website are also available for more details on the vulnerability.

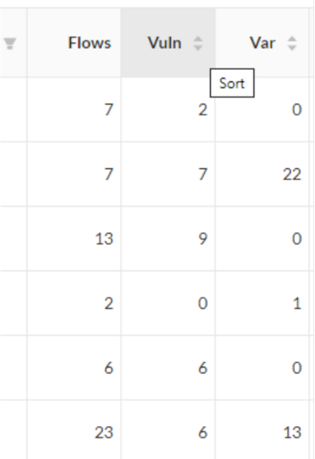
A score reports the severity of the vulnerability **(2)**. This score is calculated upon criteria from the Common Vulnerability Scoring System or CVSS. Criteria are for example the ease of attack, its impacts, the importance of the component on the network, and whether actions can be taken remotely or not. The score can go from 0 to 10, with 10 being the most critical score.

You also have the option to acknowledge a vulnerability **(3)** if you don't want to be notified anymore about it. This is used for example when a PLC is detected as vulnerable but a firewall or a security module is placed ahead. The vulnerability is therefore mitigated. An acknowledgment can be canceled at any time. Vulnerabilities acknowledgment/cancelation is accessible to the Admin, Product and Operator users only.

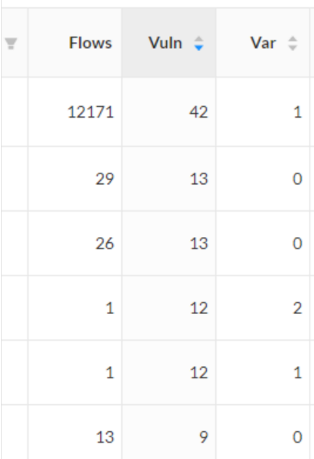
Where to find vulnerabilities?

Vulnerabilities are accessible through the Vulnerability dashboard of a preset.

Also, you can see vulnerabilities through the Device list. Sort the vulnerability column to bring vulnerable components up:

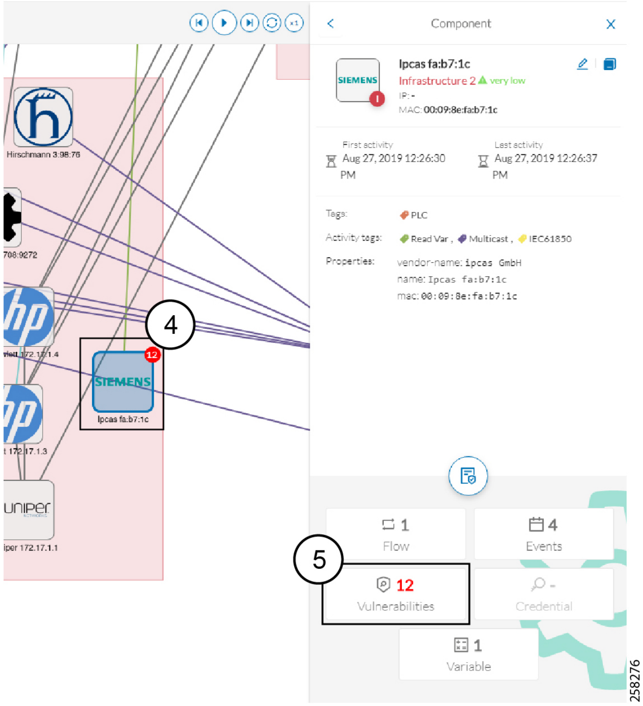


Flows	Vuln	Var
7	2	0
7	7	22
13	9	0
2	0	1
6	6	0
23	6	13



Flows	Vuln	Var
12171	42	1
29	13	0
26	13	0
1	12	2
1	12	1
13	9	0

Moreover, vulnerabilities are pointed out in the map by a device or a component with a red counter badge **(4)**. If you click it, its side panel opens on the right with the number of vulnerabilities evidenced in red **(5)**.



Component

Ipcas fa:b7:1c
Infrastructure 2 very low
IP: -
MAC: 00:09:8e:fa:b7:1c

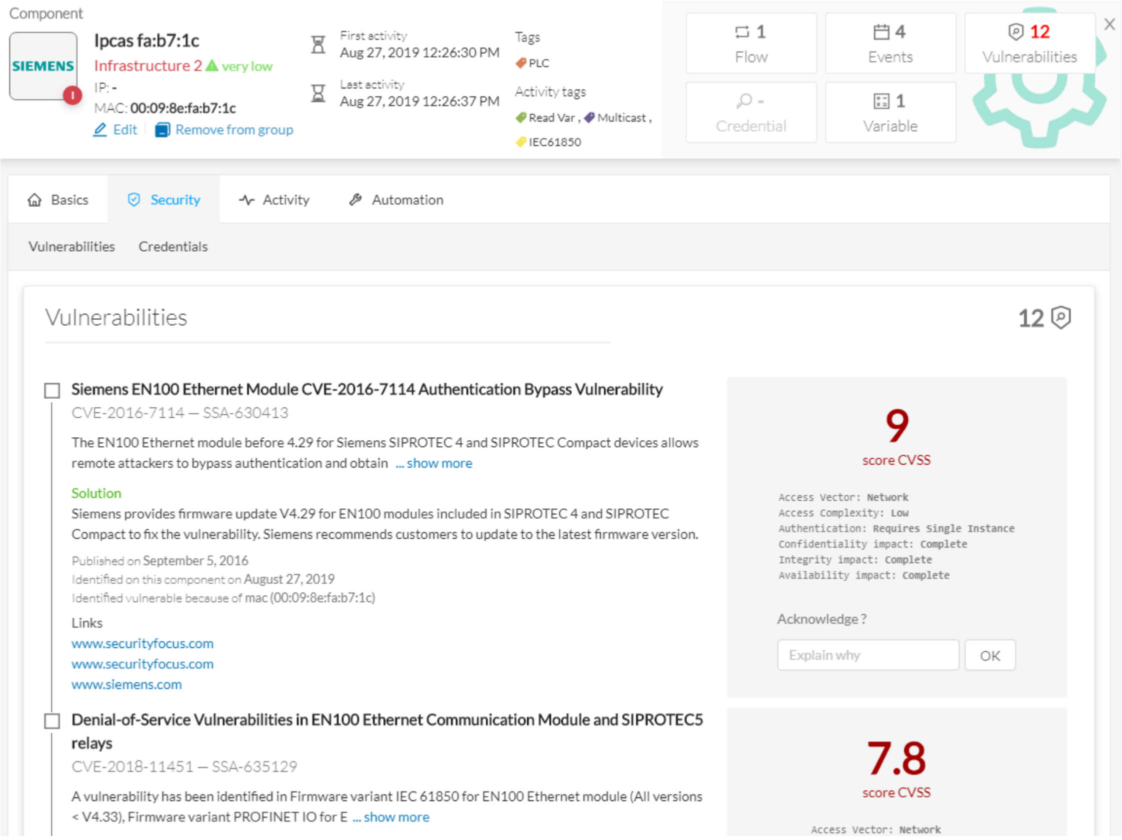
First activity
Aug 27, 2019 12:26:30 PM

Last activity
Aug 27, 2019 12:26:37 PM

Tags: PLC
Activity tags: Read Var , Multicast , IEC61850
Properties:
vendor-name: `ipcas GmbH`
name: `Ipcas fa:b7:1c`
mac: `00:09:8e:fa:b7:1c`

1 Flow
4 Events
12 Vulnerabilities
- Credential
1 Variable

Clicking the vulnerabilities displayed in red **(5)** (in the figure above) opens the device or component's technical sheet with further details about all its vulnerabilities:



Component

Ipcas fa:b7:1c
Infrastructure 2 ⚠ very low
IP: -
MAC: 00:09:8e:fa:b7:1c
Edit | Remove from group

First activity
Aug 27, 2019 12:26:30 PM
Last activity
Aug 27, 2019 12:26:37 PM

Tags
PLC
Activity tags
Read Var , Multicast ,
IEC61850

Vulnerabilities 12

□ **Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability**
CVE-2016-7114 — SSA-630413

The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain ... show more

Solution
Siemens provides firmware update V4.29 for EN100 modules included in SIPROTEC 4 and SIPROTEC Compact to fix the vulnerability. Siemens recommends customers to update to the latest firmware version.

Published on September 5, 2016
Identified on this component on August 27, 2019
Identified vulnerable because of mac (00:09:8e:fa:b7:1c)

Links
www.securityfocus.com
www.securityfocus.com
www.siemens.com

9
score CVSS

```
Access Vector: Network
Access Complexity: Low
Authentication: Requires Single Instance
Confidentiality impact: Complete
Integrity impact: Complete
Availability impact: Complete
```

Acknowledge ?
Explain why | OK

□ **Denial-of-Service Vulnerabilities in EN100 Ethernet Communication Module and SIPROTEC5 relays**
CVE-2018-11451 — SSA-635129

A vulnerability has been identified in Firmware variant IEC 61850 for EN100 Ethernet module (All versions < V4.33), Firmware variant PROFINET IO for E ... show more

7.8
score CVSS

```
Access Vector: Network
```

However, you'll be notified each time a device or component is detected as vulnerable by an event. One event is generated per vulnerable component. An event is also generated each time a vulnerability is acknowledged or not vulnerable anymore.