Vulnerability

- Vulnerability, on page 1

Vulnerability

Definition of Vulnerabilities

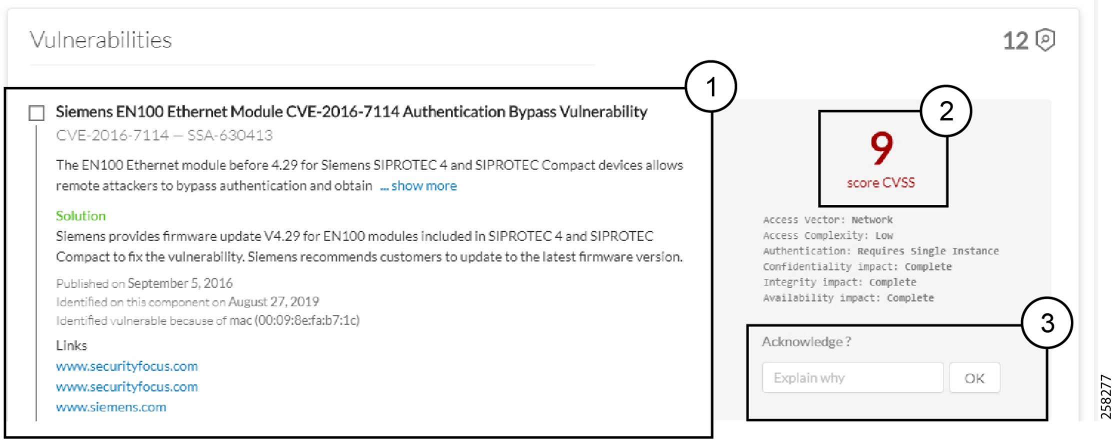
Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

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

Important Always update the Knowledge database in Cisco Cyber Vision as soon as possible after notification of a new version. This protects your network against vulnerabilities. Refer to the corresponding documentation.

Vulnerability Use

Below is an example of a Siemens component's vulnerability. See the technical sheet, Security tab.



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 ?

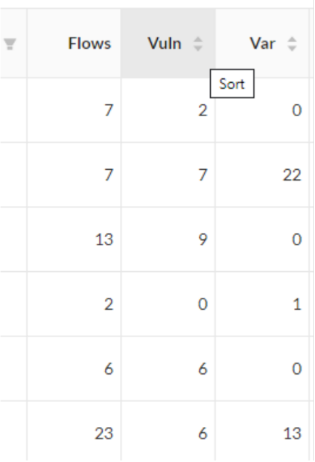
Explain why

OK

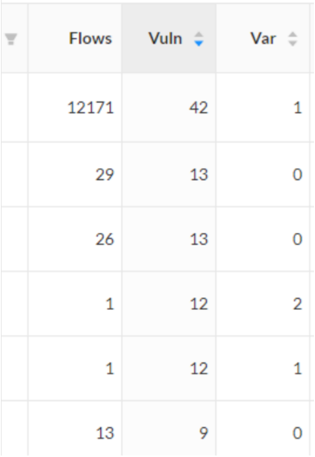
1. **Information** displayed about vulnerabilities includes the following: vulnerability type and reference, possible consequences, and solutions or actions to take on the network. Often, upgrading the device firmware alleviates a vulnerability. Links to the manufacturer website are also available.
2. A **score** reports the severity of the vulnerability. The score is calculated upon criteria from the Common Vulnerability Scoring System (CVSS). Criteria examples are: the ease of attack, its impacts, the importance of the component on the network, and whether actions can be taken remotely or not. Scores range from 0 to 10, with 10 being the most critical score.
3. **Acknowledge** a vulnerability if you don't want to be notified about it anymore. For example: a PLC is detected as vulnerable but a firewall or a security module is placed ahead. The vulnerability is mitigated. Cancel an **Acknowledgment** at any time. Only the Admin, Product, and Operator users can access **Vulnerabilities Acknowledgment/Cancelation**.

Vulnerability Location

Access Vulnerabilities in any of the following ways: click **Explore** > **All Data** > **Vulnerabilities**, use Vulnerability dashboard of a preset, or through the **Device list**. Use the **Sort arrows** to view the vulnerability column.

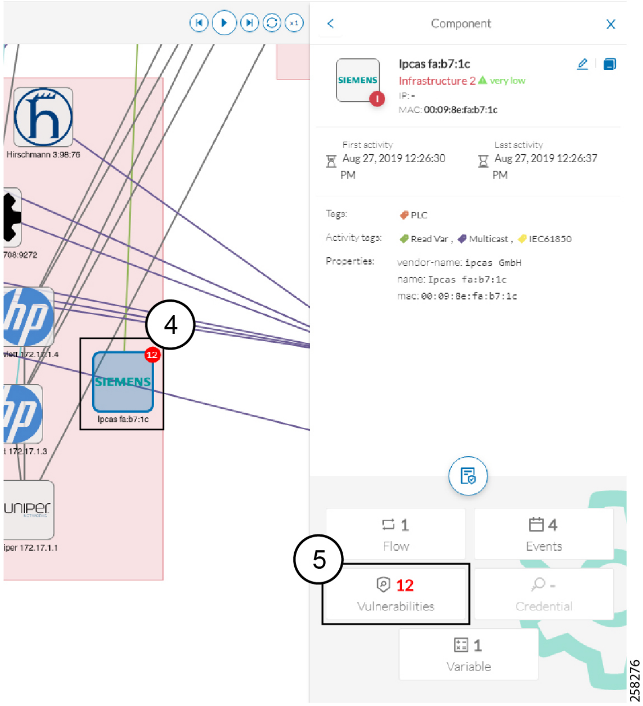


Flows	Vuln	Var
7	2	0
7	7	22
13	9	0
2	0	1
6	6	0
23	6	13



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

Find vulnerabilities on the map by a device or a component with a red counter badge. Click the badge **(4)** and the side panel opens with the number of vulnerabilities shown in red.



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

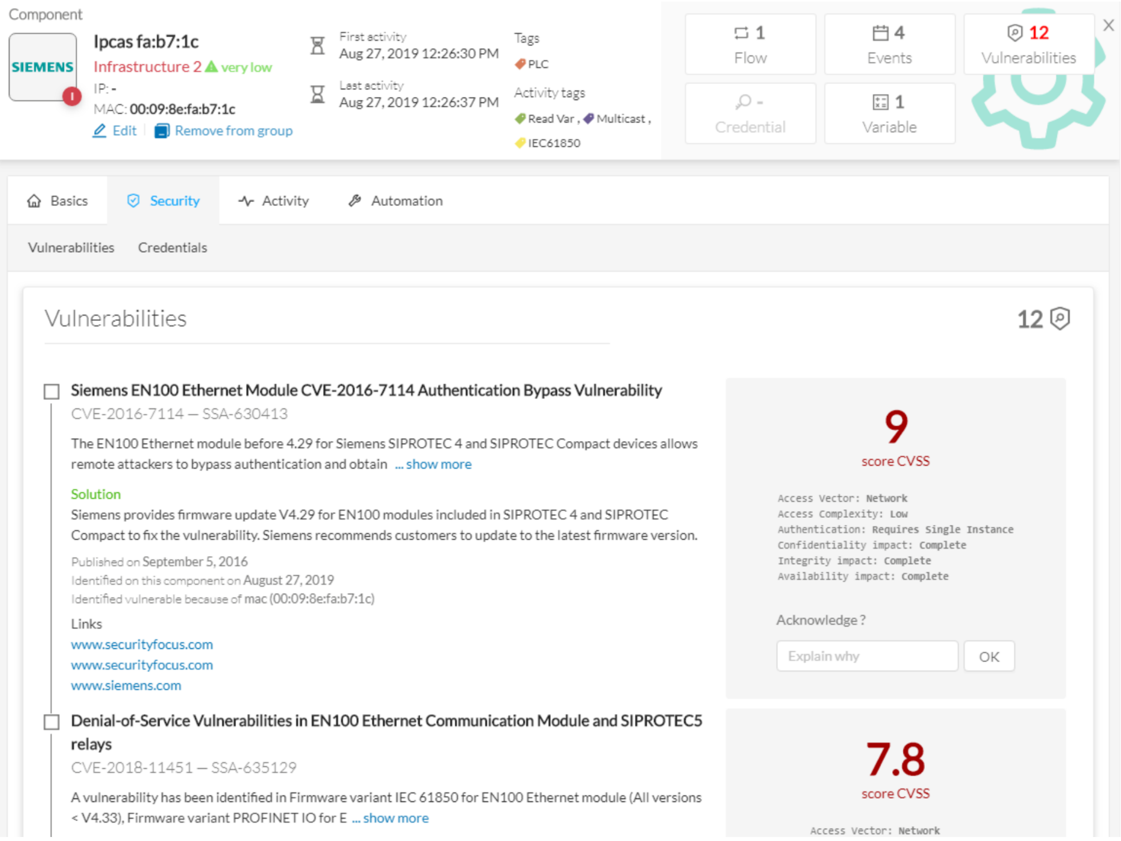
Tags: PLC

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

Click the **Vulnerabilities** in red **(5)** and the device or component's technical sheet opens.



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

1 Flow | 4 Events | 12 Vulnerabilities | - Credential | 1 Variable

Basics | Security | Activity | Automation

Vulnerabilities | Credentials

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
```

Events

An event occurs if a device or component gets detected as vulnerable. You receive a notification. One event is generated per vulnerable component. An event is also generated each time a vulnerability is acknowledged or not vulnerable anymore.