Release Notes for Cisco Cyber Vision Release 3.1.1

Compatible device list

Center	Description
VMWare ESXi OVA center	VMWare ESXi 6.x or later
Windows Server Hyper-V VHDX center	Microsoft Windows Server Hyper-V version 2016 or later
Cisco UCS C220 M5 Rack Server	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server)
Sentryo CENTER10	Sentryo CENTER10 hardware appliance
Sentryo CENTER30	Sentryo CENTER30 hardware appliance
Sensor	**Description**
Cisco IC3000	Cyber Vision Sensor hardware appliance
Cisco Catalyst IE3400	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
Cisco IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst 9300, 9400, 9500	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9400, 9500 Series switches
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Links

Software Download

https://software.cisco.com/download/home/286325414/type

The files below can be find following this link.

Center	Description
CiscoCyberVision-3.1.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-3.1.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.1.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.1.1.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-IC3K-3.1.1.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.1.tar	Cat9x00 sensor installation and update file
Updates	**Description**
CiscoCyberVision-update-center-3.1.1.dat	Center update file
CiscoCyberVision-update-sensor-3.1.1.dat	Sentryo Sensor3, 5, 7 update file
CiscoCyberVision-update-combined-3.1.1.dat	Center and Legacy Sensor update file from GUI
CiscoCyberVision-Embedded-KDB-3.1.1.dat	KnowledgeBase embedded in Cisco Cyber Vision 3.1.1

Related Documentation

New!

Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identify Services Engine via pxGrid, Release 3.1.0:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf

- Cisco Cyber Vision GUI User Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_Release_3_1_0.pdf

- Cisco Cyber Vision IE3400 and Catalyst 9300 Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IE3400_and_CAT9300_Installation_Guide_Release_3_1_0.pdf

- Cisco Cyber Vision IR1101 Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IR1101_Installation_Guide_Release_3_1_0.pdf

- Cisco Cyber Vision Sensor Quickstart Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Sensor_Quickstart_Guide_Release_3_0_0.pdf

- Cisco Cyber Vision IC3000 Troubleshooting Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IC3000_Troubleshooting_Guide_Release_3_0_2.pdf

- Cisco Cyber Vision Center Appliance Quickstart Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_Appliance_Quickstart_Guide_Release_3_0_0.pdf

- Cisco Cyber Vision Center VM Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_Release_3_0_1.pdf

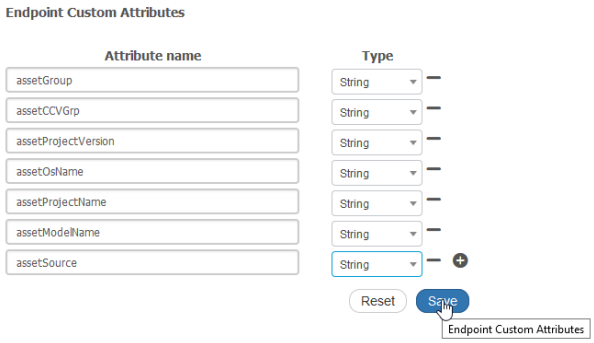
Cisco Cyber Vision new features and improvements

Add source “CCV” to identify assets coming from Cisco Cyber Vision in ISE

A new custom attribute is now exported from Cisco Cyber Vision to Cisco “Identity Services Engine (ISE)” through pxGrid. This new attribute will be used to know from where the asset comes (either Cyber Vision or another system).

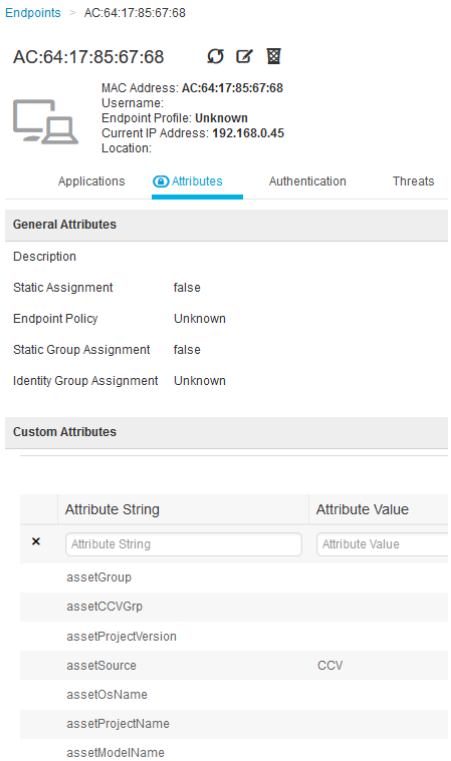
This attribute is called “assetSource”, and needs to be defined in Cisco ISE.

List of custom attributes to define in Cisco ISE:



Once configured, Cisco ISE will add the value CCV in the custom attribute called assetCCVGroup if the endpoint is coming from Cisco Cyber Vision:

Cisco ISE, endpoint details:



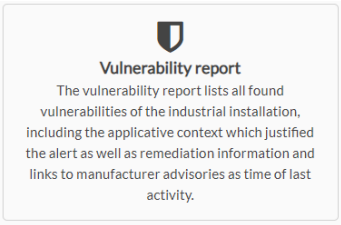
Performance improvements

Several services in Cisco Cyber Vision were improved to fix performance issues. Concurrent access to the database due to events and variables in the case of large system are now more efficient.

Add CVE columns in “Vulnerability Database”

The Cisco Cyber Vision vulnerability database contained in the vulnerability report now shows a CVE column.

Cisco Cyber Vision Vulnerability report link



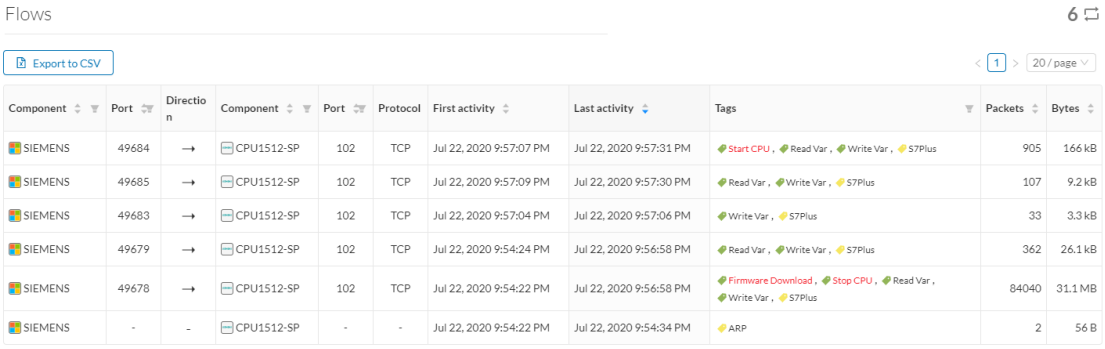
New CVE column in the Vulnerability Database tab:

Title	CVSS	CVSS Tem	CVE	Summary
Information Disclosure Vulnerability in the OZW Web Server	0	0	CVE-2019-13941	Vulnerable versions of OZW Web Server use
Vulnerabilities in SIMATIC S7-1200 and SIMATIC S7-1500 CPU families	4.3	0	CVE-2019-10929	A vulnerability has been identified in SIMAT
Rockwell Automation MicroLogix 1400 Controllers - Stack Buffer Overflow Vulnerability	7.5	0	CVE-2017-16740	A Buffer Overflow issue was discovered in R
Improper Authentication Vulnerability in MS3000 Migration Server	0	0	CVE-2019-18312	An attacker with network access to the MS3
Multiple vulnerabilities in Modicon Controllers	0	0	CVE-2019-6830	Uncaught Exception vulnerability exists whi
Siemens Security Advisory SSA-321046 - CVE-2014-8479	6.8	0	CVE-2014-8479	The FTP server on Siemens SCALANCE X-30
Siemens SINAMICS PERFECT HARMONY GH180 Drives NXG I and NXG II - Denial Of Serv	5	0	CVE-2019-6578	A vulnerability has been identified in SINAM
Vulnerabilities in Intel CPUs	0	0	CVE-2019-0169	Heap overflow in subsystem in Intel(R) CSM
Rockwell Automation Allen-Bradley MicroLogix 1100 and 1400 - Multiple Flaws	5	0	CVE-2017-7899	An Information Exposure issue was discover

CSV exports now handle filters and sorting

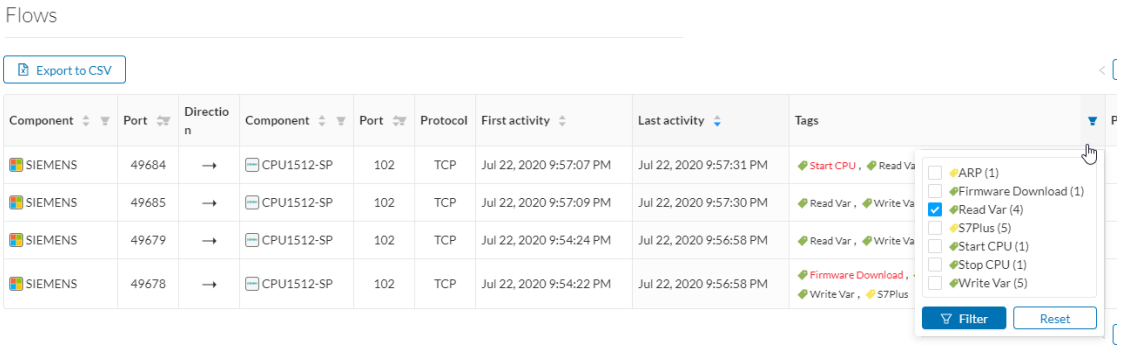
The Cisco Cyber Vision Center now exports only visible flows when they are exported as CSV.

Unfiltered flows:



Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Tags	Packets	Bytes
SIEMENS	49684	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:57:07 PM	Jul 22, 2020 9:57:31 PM	Start CPU, Read Var, Write Var, S7Plus	905	166 kB
SIEMENS	49685	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:57:09 PM	Jul 22, 2020 9:57:30 PM	Read Var, Write Var, S7Plus	107	9.2 kB
SIEMENS	49683	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:57:04 PM	Jul 22, 2020 9:57:06 PM	Write Var, S7Plus	33	3.3 kB
SIEMENS	49679	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:54:24 PM	Jul 22, 2020 9:56:58 PM	Read Var, Write Var, S7Plus	362	26.1 kB
SIEMENS	49678	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:54:22 PM	Jul 22, 2020 9:56:58 PM	Firmware Download, Stop CPU, Read Var, Write Var, S7Plus	84040	31.1 MB
SIEMENS	-	-	CPU1512-SP	-	-	Jul 22, 2020 9:54:22 PM	Jul 22, 2020 9:54:34 PM	ARP	2	56 B

Filtered flows:



Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Tags
SIEMENS	49684	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:57:07 PM	Jul 22, 2020 9:57:31 PM	Start CPU, Read Va
SIEMENS	49685	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:57:09 PM	Jul 22, 2020 9:57:30 PM	Read Var, Write Va
SIEMENS	49679	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:54:24 PM	Jul 22, 2020 9:56:58 PM	Read Var, Write Va
SIEMENS	49678	→	CPU1512-SP	102	TCP	Jul 22, 2020 9:54:22 PM	Jul 22, 2020 9:56:58 PM	Firmware Download, Write Var, S7Plus

CSV file with exported flows limited to the filtered flows:

Component 1 - Name	Component 1 - Port	Direction	Component 2 - Name	Component 2 - Port	Protocol	First Activity	Tags	Packets	Bytes
SIEMENS	49684	→	CPU1512-SP	102	TCP	2020-07-22 19:57:07.738 +0000 UTC	Read Var/S7Plus/Start CPU/Write Var	905	165603
SIEMENS	49685	→	CPU1512-SP	102	TCP	2020-07-22 19:57:09.459 +0000 UTC	Read Var/S7Plus/Write Var	107	9199
SIEMENS	49679	→	CPU1512-SP	102	TCP	2020-07-22 19:54:24.251 +0000 UTC	Read Var/S7Plus/Write Var	362	26095
SIEMENS	49678	→	CPU1512-SP	102	TCP	2020-07-22 19:54:22.997 +0000 UTC	Firmware Download/Read Var/S7Plus/Stop CPU/Write Var	84040	31054387

Extend monitor mode syslog export

Cisco Cyber Vision syslog events linked to baseline differences are now improved. In addition to a general event with the number of new differences, some new syslog events are generated when:

- A new component is discovered
- A new activity is discovered
- A new component tag is added
- A new component property is populated
- A modified component property appears
- A new activity is discovered
- A new activity tag is added
- A new variable access is discovered

In example for a firmware change:

Message: CEF:0|sentryo|cybervision|1.0|baseline_differences|Differences detected on a Baseline|2|cat=Anomaly Detection msg=Property fw-version of component Siemens 81:21:3d on baseline ALL has been modified from V2.8.1 to V2.6.1 SCVBaselineId=ea0d7535-c852-49b2-bb18-bd8f6b5b9146 SCVBaselineName=ALL SCVComponentId=0fc084f0-35e7-5155-a46b-284ee083a091 SCVComponentName=Siemens 81:21:3d SCVDifferenceId=58069c23-41ee-4c53-aed9-c40e8a554ce9 SCVDifferencePropertyName=fw-version SCVDifferencePropertyOldValue=V2.8.1 SCVDifferencePropertyValue=V2.6.1 SCVDifferenceType=modified_component_properties SCVPresetName=All data

In example for a new component:

Message: CEF:0|sentryo|cybervision|1.0|baseline_differences|Differences detected on a Baseline|2|cat=Anomaly Detection msg=New component Vmware d2:45:53 has been detected on baseline ALL SCVBaselineId=ea0d7535-c852-49b2-bb18-bd8f6b5b9146 SCVBaselineName=ALL SCVComponentId=7e1792d8-9d0b-5a74-8936-644ee2fcd886 SCVComponentName=Vmware d2:45:53 SCVDifferenceId=7de0f94e-97cc-4955-b20b-46b84c19dab8 SCVDifferenceType=new_component SCVPresetName=All data

In example for a new activity:

Message: CEF:0|sentryo|cybervision|1.0|baseline_differences|Differences detected on a Baseline|2|cat=Anomaly Detection msg=New activity '216.239.35.0 CPU1512-SP' has been detected on baseline PLCs SCVActivityComponentAId=74d6641b-eb59-500b-babb-7c70014935fb SCVActivityComponentAName=216.239.35.0 SCVActivityComponentBId=6362bc30-4cc0-5dfa-b02f-39f1ec963bb3 SCVActivityComponentBName=CPU1512-SP SCVActivityId=083dd89a-a60f-54f1-93e1-0b6b6a8c73de SCVBaselineId=a0ef192f-48ad-4419-8340-8115510183a0 SCVBaselineName=PLCs SCVDifferenceId=162527c8-7b94-49ef-af0e-342648acf472 SCVDifferenceType=new_activity SCVPresetName=ERIC

Generate event on sensor low resources

Optional feature in release 3.1.1, the Cisco Cyber Vision Center generates some events on sensor low resources. A configuration file is needed to define thresholds and to enable this functionality.

Configuration file called “sysinfod-sensor-handler.conf” localized in the center (/data/etc/sbs/).

```
# /data/etc/sbs/sysinfod-sensor-handler.conf
enable_sensor_ressources_events: true
cpu_threshold: 80
memory_threshold: 80
disk_theshold: 80
threshold_check_period: 600
```

Cyber Vision event:

CEF format syslog event:

Message: CEF:0|sentryo|cybervision|1.0|sensor_high_ressources|Sensor high ressources usage|1|cat=Cisco Cyber Vision Administration msg=Sensor [Name: , IP: 192.168.69.29] high usage of ressources: CPU [31% >\= 30%], Memory [22% >\= 20%] SCVEventType=sensor SCVSensorAction=high ressources usage SCVSensorCpu=31 SCVSensorDisk=0 SCVSensorId=2a18454c-0fcc-4d47-94ab-fa1900cf3d0a SCVSensorIp=192.168.69.29 SCVSensorMemory=22 SCVSensorName=unknown SCVSensorTime=2020-07-21T11:17:00Z SCVSensorVersion=3.1.1+202007210201

Improve some syslog events with the addition of the Sensor ID

Events related to flow like new flow, new component, new properties, … are now sent to syslog with a new field called “SCVSensorId”.

Example of a new component:

Message: CEF:0|sentryo|cybervision|1.0|component_new|New component detected|2|cat=Inventory Events msg=New component detected on the network: IP 192.168.0.169, MAC 70:e4:22:a0:fa:40, vendor Cisco src=192.168.0.169 smac=70:e4:22:a0:fa:40 SCVEventType=new_component SCVComponentId=85702eff-c395-5746-af3e-7a8c60e60371 SCVComponentName=Unnamed component SCVSensorId=e7d38ca4-8fc2-4abc-8d39-83228797fd48

For a property change

Message: CEF:0|sentryo|cybervision|1.0|component_properties_change|Changed properties on a component detected|1|cat=Inventory Events msg=Normalized properties have changed: vendor-name\="Siemens" cmp-a-mac=01:80:c2:00:00:0e cmp-b-mac=ac:64:17:85:67:6a cmp-a= cmp-b= cmp-a-port=0 cmp-b-port=0 SCVEventType=changed_properties SCVComponentId=d9677955-49f5-5494-828a-9f07f63e15c4 SCVComponentName=hmixb110d0 SCVComponentProperties0Name=vendor-name SCVComponentProperties0Value=Siemens SCVComponentPropertiesNumber=1 SCVSensorId=e7d38ca4-8fc2-4abc-8d39-83228797fd48

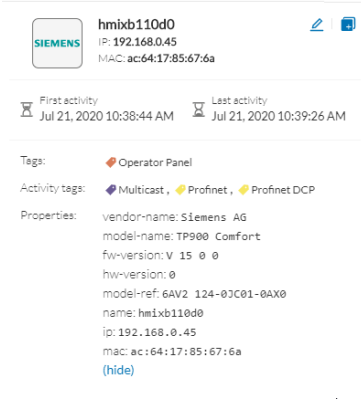
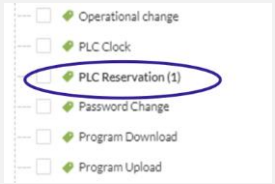
For a new flow:

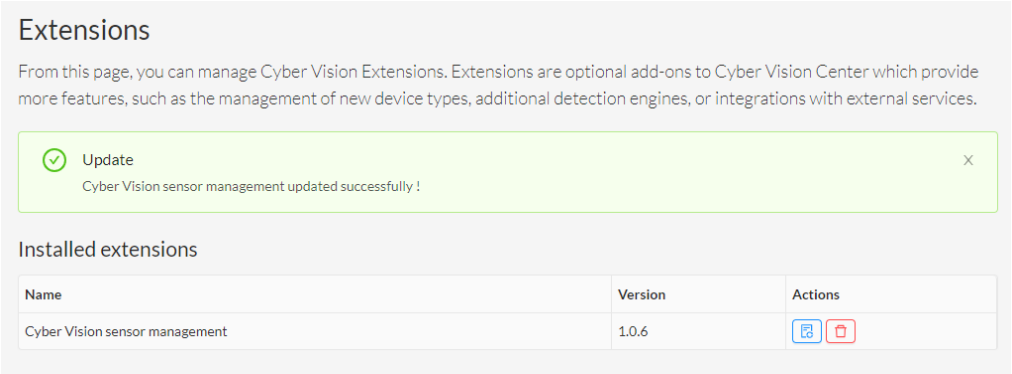
Message: CEF:0|sentryo|cybervision|1.0|communication_new|New communication|2|cat=Security Events msg=New Ethernet/IP communication has been detected between 192.168.0.121:44818 and 192.168.0.154:50039 cmp-a-mac=70:e4:22:a0:fa:40 cmp-b-mac=d0:ec:35:ca:00:4a cmp-a=192.168.0.121 cmp-b=192.168.0.154 cmp-a-port=44818 cmp-b-port=50039 SCVEventType=flow_new SCVFlowCmpAComponentId=acc66511-5ba7-54ab-ad87-531332de930c SCVFlowCmpAComponentName= SCVFlowCmpBComponentId=226ce04f-597d-5606-a6e6-8ff707294d6e SCVFlowCmpBComponentName= SCVFlowCommunicationType=Ethernet/IP SCVFlowId=6e95a2f4-e4fb-5388-a01e-e58de265e221 SCVSensorId=e7d38ca4-8fc2-4abc-8d39-83228797fd48

Improve Diagnostic files

Results of the command sbs-diag were improved. Additional information was added to cover more services in the product.

Cisco Cyber Vision Bug fixed

Issues ID / CDETS	Description
#1667 /	Fix french translation in search by filter of event calendar 
#2482 /	Improve UMAS decoding
#2494 / CSCvs21855, CSCvs47253	Login to sensor app does not work with the password set unless it is rebooted once
#3419 /	Add a LowVolume tag whitelist
#3508 /	Missing normalized properties of the component found in the LLDP properties (ie. Siemens TP900) 
#3668 /	MMS – Add tag “PLC_RESERVATION” 
#3762 /	Monitor mode - Focus the most relevant tab when reviewing differences
#3963 /	Fix inconsistent criteria filtering results - Filters was no consistent, with the same 'ticked'/unticked items depending on timing, the result was different.
#4167 /	Fix search with special characters

Issues ID / CDETS	Description
#4204 /	Correction of the upgrade alert message in the sensor management extension page 
#4228 /	Fix flows table sorting of “First activity” and “Last activity” columns
#4284 /	Fix command “sbs db reclaim-disk-space" that was returning an error
#4391 /	Fix “Investigate in CTR” button redirection URL after setting CTR platform value
#4423 / CSCvu61111	DNP3 – Add variable write access when variable is written with Direct Operate No ACK
#4428 /	Fix sbs-db purge-flow command, which was giving some errors
#4439 /	Fix the management of caravan rules when multiple rules/protocols exist for the same port
#4423 / CSCvu61111	DNP3 – Add variable write access when variable is written with Direct Operate No ACK
#4428 /	Fix sbs-db purge-flow command, which was giving some errors
#4439 /	Fix the management of caravan rules when multiple rules/protocols exist for the same port
#4515 /	Improve stowd performances
#4518 /	Improve Siemens LLC decoding (fix decode errors)
#4555 /	New stowd option to disable upsert into variable_access
#4557 /	New options to disable variable per protocol
#4560 /	Fix issue with Low Volume tag which could create false positive in monitor mode
#4561 /	Increase exception event aggregation to 5 minutes
#4598 / CSCvu65838	Fix Cisco CTR EMEA server URL.

Issues ID / CDETS	Description
#4715 /	Fix missing or incomplete protocol finalizers.
#4716 /	Optimize the reception of snort events by burrow
#4717 /	Optimize the reception of sysinfo by sysinfod-sensor-handler
#4833 /	Fix variable export issue when ‘max_variables = 0’
#4835 /	Fix max_variables issue causing generation of empty flows in flow tables with type variable
#4921 /	Batch the insertion of exception events
#4961 /	Fix error in IC3K offline enrollment after rebooting the device
#4988 /	Fix burrow crashes with some flow tables
#5011 /	Add an option to ignore decode errors in burrow
#5022 /	Bump bootdisk from 512MB to 1024MB
#5052 /	Increase HAProxy max number of files
#4988 /	Sync SNORT custom configuration on sensors – A script is now available.
#4249 – 4824 / CSCvu73470	Cyber Vision Center pxGrid Documentation was updated to add configuration information to facilitate the deployment. Link of this new documentation in part ‘Related Documentation’.
#5055 /	Fix baseline acknowledge error.
#4999 /	Fix infinite loop on group unlock.
#3141 /	Add an error message on group name conflict.

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
#3533 / CSCvs47260 **CSCvs47253**	IC3000 Sensor integration	• The password configuration required when generating a provisioning package for the IC3000 is sometimes not considered. Thus, login in IOx Local Manager to install the Sensor Application is refused and the procedure must be redone. • Login to IOx Local Manager won't work unless the IC3000 is rebooted once.
#3542 / CSCvt18302	pxGrid-agent	Cisco Cyber Vision pxGrid configuration fails when using white spaces in the Node Name field because this is not endured in Cisco ISE.
#3929/ CSCvt55787	pxGrid-agent	Cisco Cyber Vision Center should not send broadcast address to Cisco ISE as an endpoint using pxGrid.
#4821/ CSCvu41812	pxGrid-agent	Cisco ISE pxGrid communication goes down after upgrade and needs to be started manually.
#4397/ CSCvu47880	pxGrid-agent	Cisco Cyber Vision pxGrid update does not remove attribute from endpoint in Cisco ISE. In example if a component is removed from a group, the endpoint group name is not cleared in Cisco ISE.
#4823/ CSCvu73461	pxGrid-agent	Cisco Cyber Vision not sending customized component name to ISE
#4825/ CSCvu80175	pxGrid-agent	Cisco Cyber Vision pxGrid do not publish Stomp Updates unless reboot right after integration