QUEEN'S UNIVERSITY BELFAST

ESTᴰ 1845

CSIT

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Update on ONOS and ODL Security Comparison

DR. SANDRA SCOTT-HAYWARD, QUEEN'S UNIVERSITY BELFAST

PARIS, 17 JUNE 2019

Queen’s University Belfast – Lanyon Building

Est. 1845

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

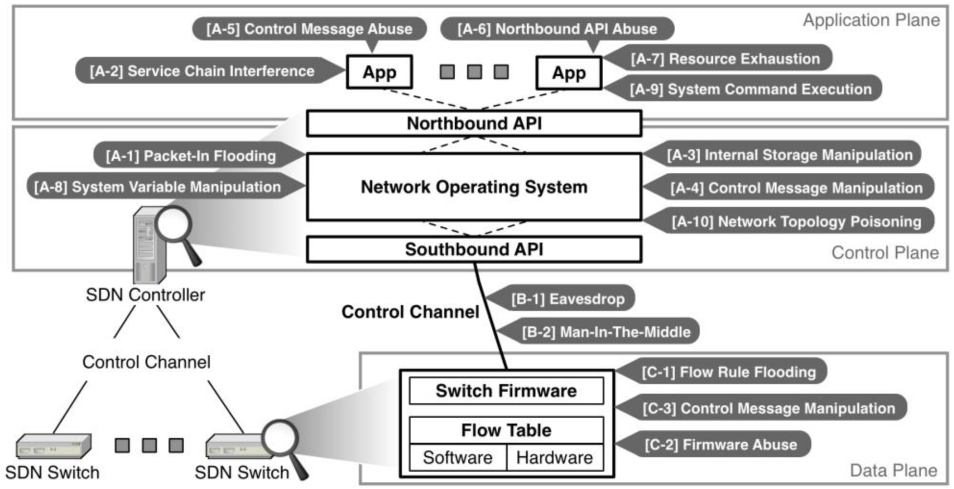
Centre for Secure Information Technologies (CSIT)

CSIT is the UK's Innovation and Knowledge Centre for Cybersecurity

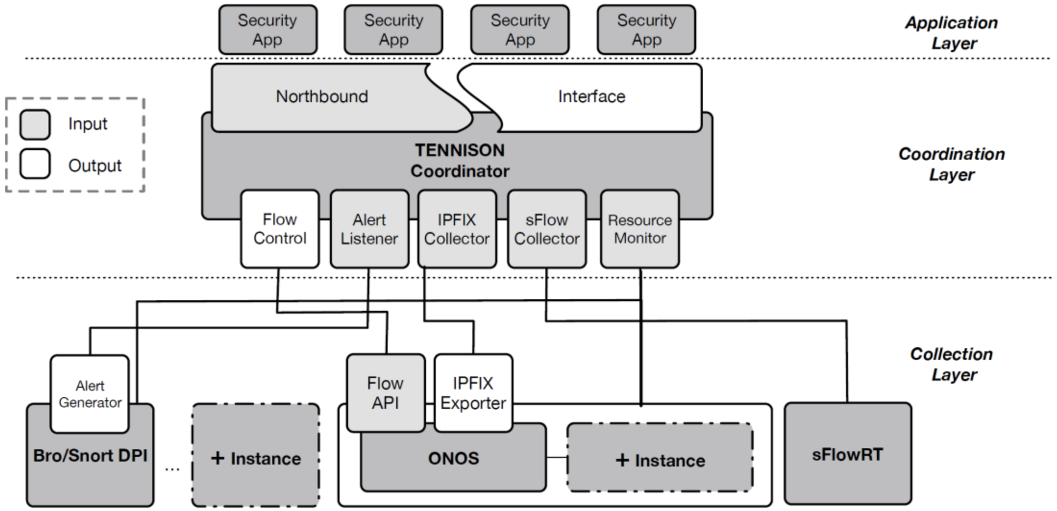
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDNFV Security Research - Objectives

Identifying, raising awareness, and recommending solutions to potential vulnerabilities in SDNFV network design and deployment.


Application Plane
[A-5] Control Message Abuse
[A-6] Northbound API Abuse
[A-2] Service Chain Interference
App
App
[A-7] Resource Exhaustion
[A-9] System Command Execution
Northbound API
[A-1] Packet-In Flooding
[A-8] System Variable Manipulation
Network Operating System
[A-3] Internal Storage Manipulation
[A-4] Control Message Manipulation
[A-10] Network Topology Poisoning
Southbound API
Control Plane
SDN Controller
Control Channel
[B-1] Eavesdrop
[B-2] Man-In-The-Middle
Control Channel
[C-1] Flow Rule Flooding
Switch Firmware
[C-3] Control Message Manipulation
Flow Table
[C-2] Firmware Abuse
Software
Hardware
SDN Switch
SDN Switch
Data Plane

Exploring scalable, analytics-based monitoring and forensics capabilities, and security solutions for these new network architectures.



Agenda for the talk

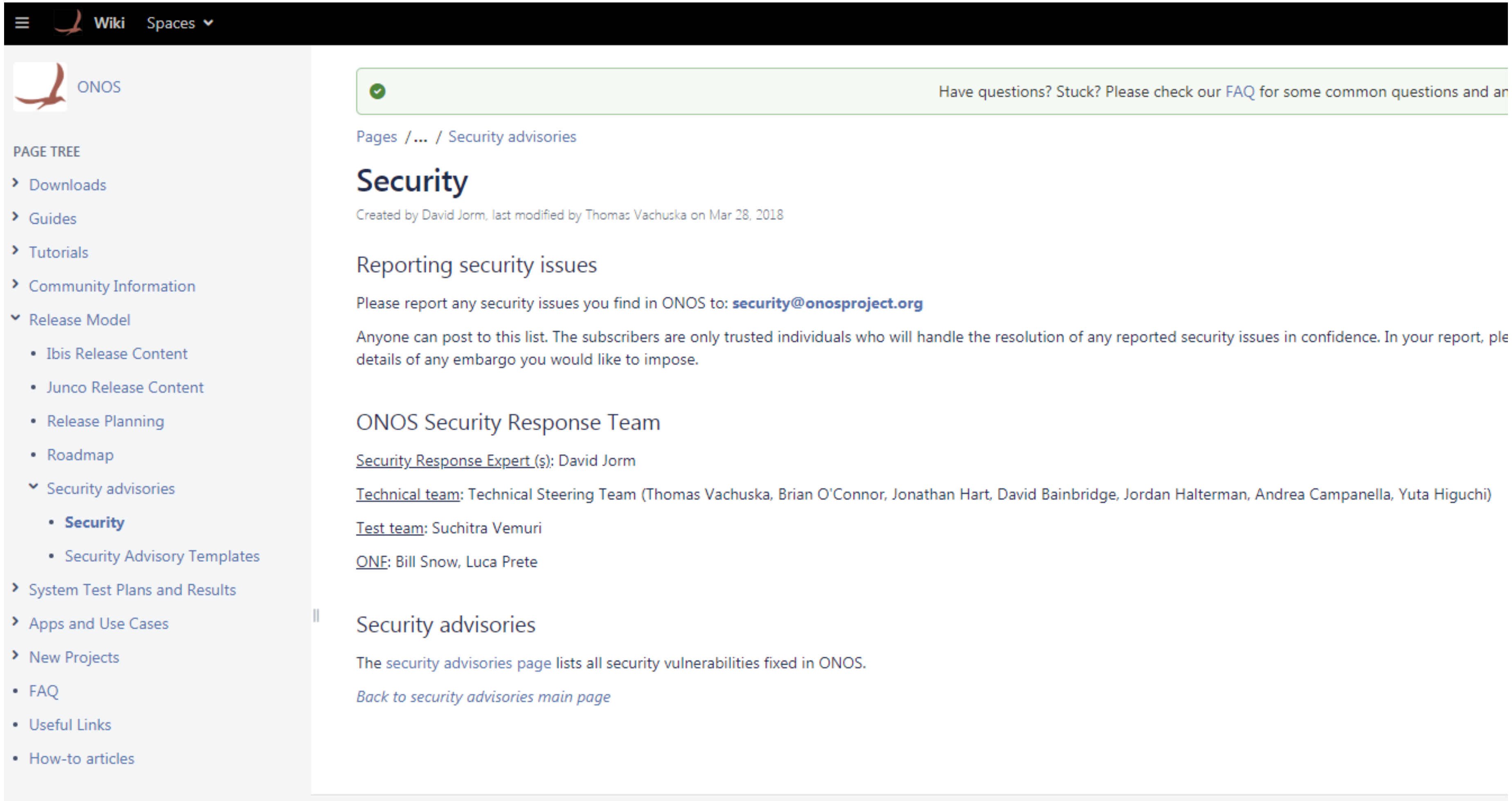
1. Security Support (ONOS/ODL)

2. Security-specific Projects/Applications (ONOS/ODL)

3. Security-focused design (ONOS/ODL)

4. Conclusion

Security Support – ONOS



Have questions? Stuck? Please check our FAQ for some common questions and ar

Pages /... / Security advisories

Security

Created by David Jorm, last modified by Thomas Vachuska on Mar 28, 2018

Reporting security issues

Please report any security issues you find in ONOS to: **security@onosproject.org**

Anyone can post to this list. The subscribers are only trusted individuals who will handle the resolution of any reported security issues in confidence. In your report, ple details of any embargo you would like to impose.

ONOS Security Response Team

Security Response Expert (s): David Jorm

Technical team: Technical Steering Team (Thomas Vachuska, Brian O'Connor, Jonathan Hart, David Bainbridge, Jordan Halterman, Andrea Campanella, Yuta Higuchi)

Test team: Suchitra Vemuri

ONF: Bill Snow, Luca Prete

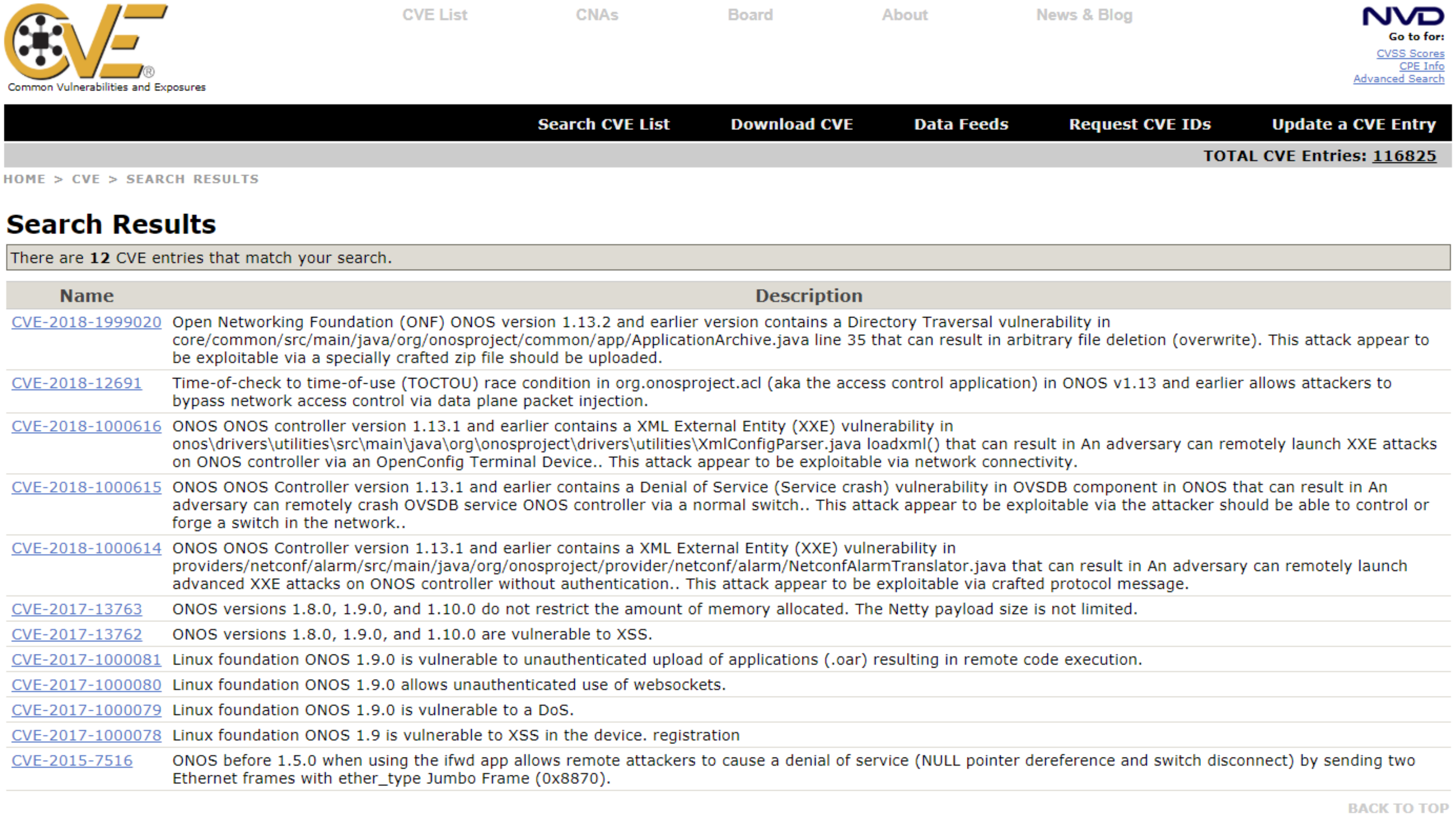
Security advisories

The security advisories page lists all security vulnerabilities fixed in ONOS.

Back to security advisories main page

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Security Support - ONOS



TOTAL CVE Entries: 116825

HOME > CVE > SEARCH RESULTS

Search Results

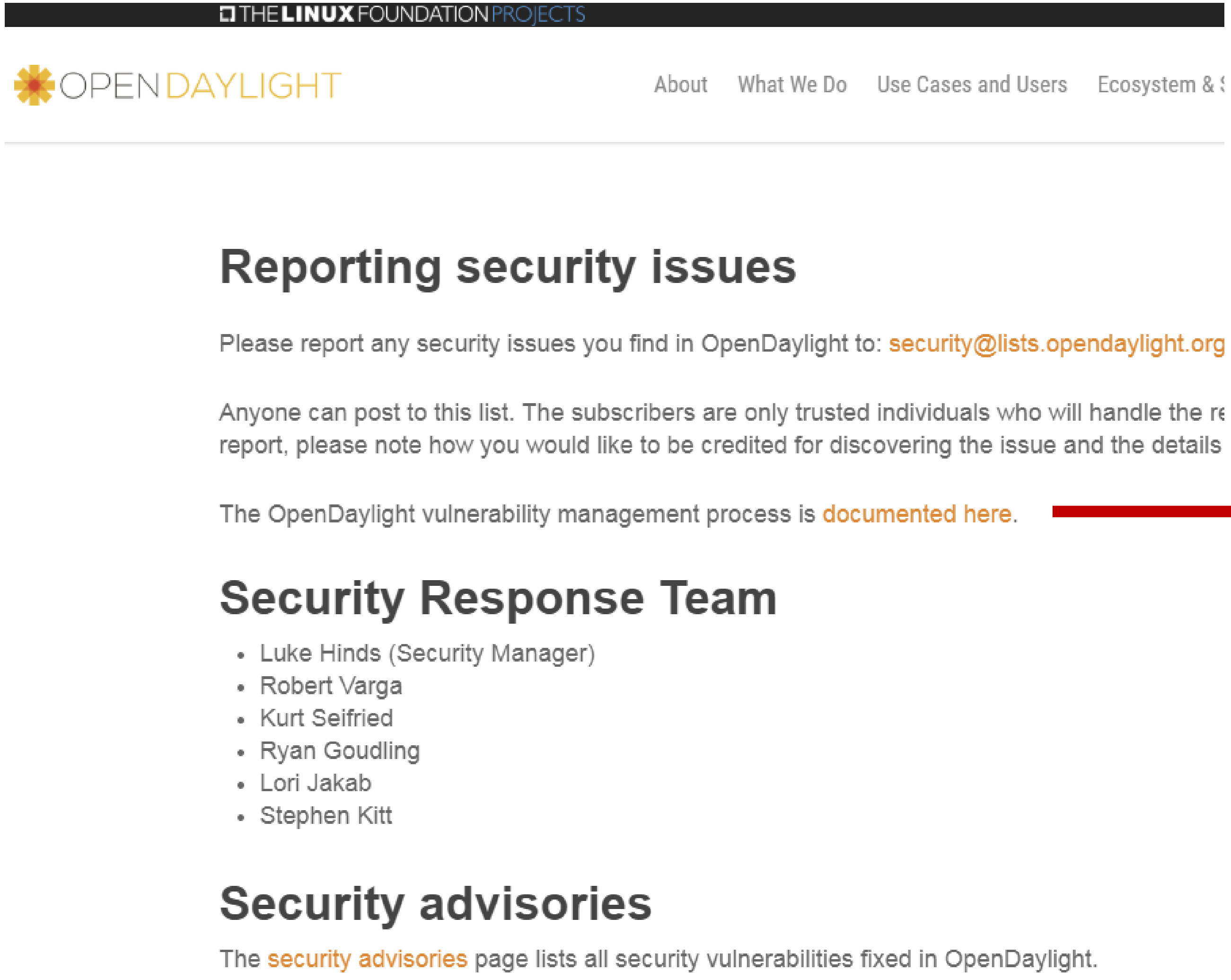
There are **12** CVE entries that match your search.

Name	Description
CVE-2018-1999020	Open Networking Foundation (ONF) ONOS version 1.13.2 and earlier version contains a Directory Traversal vulnerability in core/common/src/main/java/org/onosproject/common/app/ApplicationArchive.java line 35 that can result in arbitrary file deletion (overwrite). This attack appear to be exploitable via a specially crafted zip file should be uploaded.
CVE-2018-12691	Time-of-check to time-of-use (TOCTOU) race condition in org.onosproject.acl (aka the access control application) in ONOS v1.13 and earlier allows attackers to bypass network access control via data plane packet injection.
CVE-2018-1000616	ONOS ONOS controller version 1.13.1 and earlier contains a XML External Entity (XXE) vulnerability in onos\drivers\utilities\src\main\java\org\onosproject\drivers\utilities\XmlConfigParser.java loadxml() that can result in An adversary can remotely launch XXE attacks on ONOS controller via an OpenConfig Terminal Device.. This attack appear to be exploitable via network connectivity.
CVE-2018-1000615	ONOS ONOS Controller version 1.13.1 and earlier contains a Denial of Service (Service crash) vulnerability in OVSDB component in ONOS that can result in An adversary can remotely crash OVSDB service ONOS controller via a normal switch.. This attack appear to be exploitable via the attacker should be able to control or forge a switch in the network..
CVE-2018-1000614	ONOS ONOS Controller version 1.13.1 and earlier contains a XML External Entity (XXE) vulnerability in providers/netconf/alarm/src/main/java/org/onosproject/provider/netconf/alarm/NetconfAlarmTranslator.java that can result in An adversary can remotely launch advanced XXE attacks on ONOS controller without authentication.. This attack appear to be exploitable via crafted protocol message.
CVE-2017-13763	ONOS versions 1.8.0, 1.9.0, and 1.10.0 do not restrict the amount of memory allocated. The Netty payload size is not limited.
CVE-2017-13762	ONOS versions 1.8.0, 1.9.0, and 1.10.0 are vulnerable to XSS.
CVE-2017-1000081	Linux foundation ONOS 1.9.0 is vulnerable to unauthenticated upload of applications (.oar) resulting in remote code execution.
CVE-2017-1000080	Linux foundation ONOS 1.9.0 allows unauthenticated use of websockets.
CVE-2017-1000079	Linux foundation ONOS 1.9.0 is vulnerable to a DoS.
CVE-2017-1000078	Linux foundation ONOS 1.9 is vulnerable to XSS in the device. registration
CVE-2015-7516	ONOS before 1.5.0 when using the ifwd app allows remote attackers to cause a denial of service (NULL pointer dereference and switch disconnect) by sending two Ethernet frames with ether_type Jumbo Frame (0x8870).

BACK TO TOP

2015 – 1 CVE
2017 – 6 CVEs
2018 – 5 CVEs

Security Support - ODL



Reporting security issues

Please report any security issues you find in OpenDaylight to: security@lists.opendaylight.org

Anyone can post to this list. The subscribers are only trusted individuals who will handle the re report, please note how you would like to be credited for discovering the issue and the details

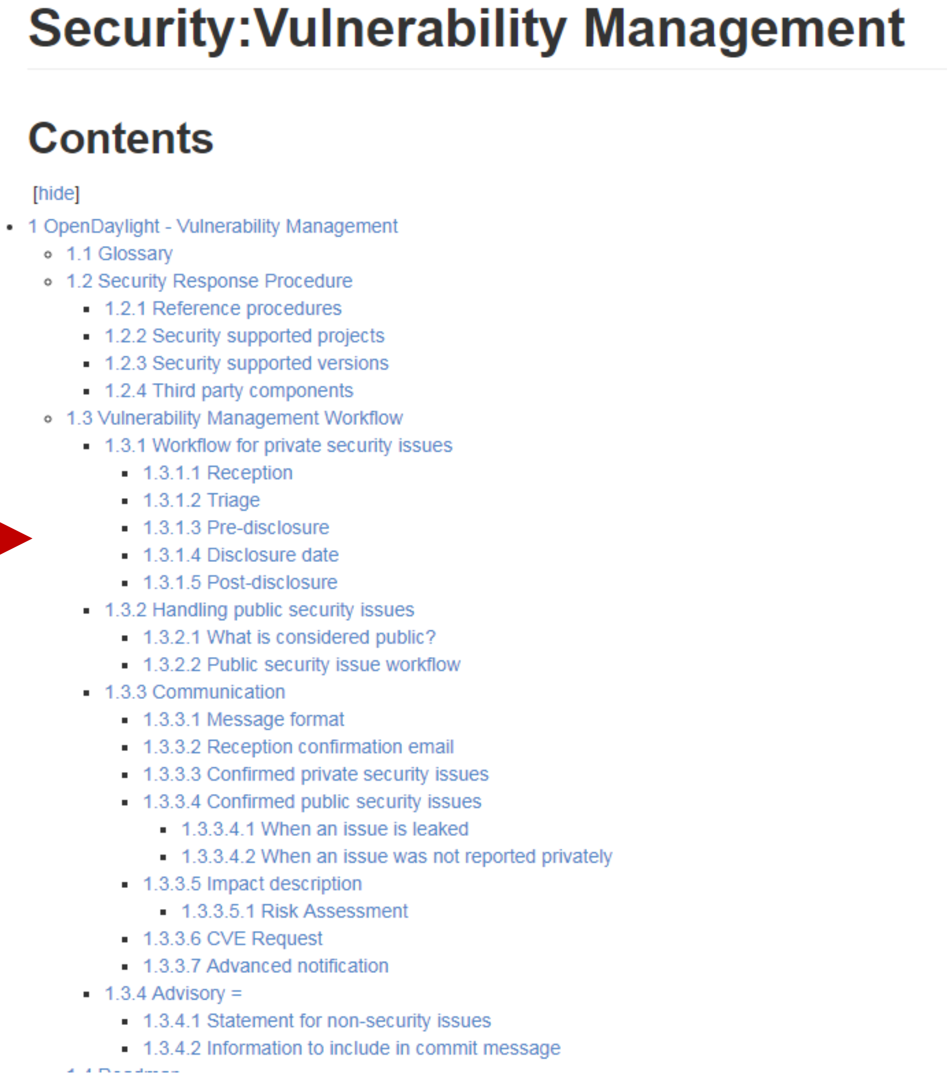
The OpenDaylight vulnerability management process is documented here.

Security Response Team

- Luke Hinds (Security Manager)
- Robert Varga
- Kurt Seifried
- Ryan Goudling
- Lori Jakab
- Stephen Kitt

Security advisories

The security advisories page lists all security vulnerabilities fixed in OpenDaylight.



Security:Vulnerability Management

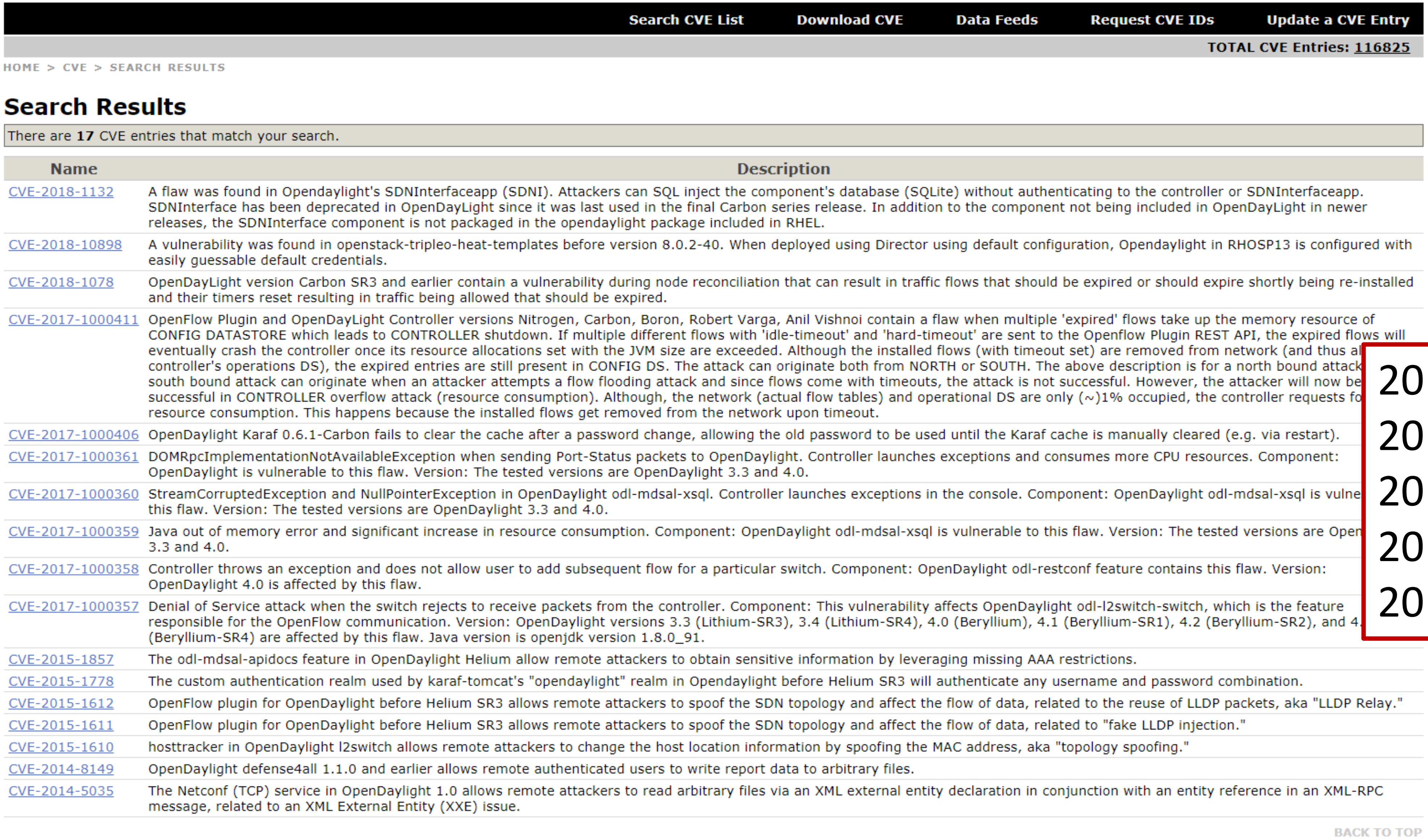
Contents

[hide]

- 1 OpenDaylight - Vulnerability Management
  - 1.1 Glossary
  - 1.2 Security Response Procedure
    - 1.2.1 Reference procedures
    - 1.2.2 Security supported projects
    - 1.2.3 Security supported versions
    - 1.2.4 Third party components
  - 1.3 Vulnerability Management Workflow
    - 1.3.1 Workflow for private security issues
      - 1.3.1.1 Reception
      - 1.3.1.2 Triage
      - 1.3.1.3 Pre-disclosure
      - 1.3.1.4 Disclosure date
      - 1.3.1.5 Post-disclosure
    - 1.3.2 Handling public security issues
      - 1.3.2.1 What is considered public?
      - 1.3.2.2 Public security issue workflow
    - 1.3.3 Communication
      - 1.3.3.1 Message format
      - 1.3.3.2 Reception confirmation email
      - 1.3.3.3 Confirmed private security issues
      - 1.3.3.4 Confirmed public security issues
        - 1.3.3.4.1 When an issue is leaked
        - 1.3.3.4.2 When an issue was not reported privately
      - 1.3.3.5 Impact description
        - 1.3.3.5.1 Risk Assessment
      - 1.3.3.6 CVE Request
      - 1.3.3.7 Advanced notification
    - 1.3.4 Advisory =
      - 1.3.4.1 Statement for non-security issues
      - 1.3.4.2 Information to include in commit message

Security Support - ODL

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES



Search Results

There are **17** CVE entries that match your search.

Name	Description
CVE-2018-1132	A flaw was found in Opendaylight's SDNInterfaceapp (SDNI). Attackers can SQL inject the component's database (SQLite) without authenticating to the controller or SDNInterfaceapp. SDNInterface has been deprecated in OpenDayLight since it was last used in the final Carbon series release. In addition to the component not being included in OpenDayLight in newer releases, the SDNInterface component is not packaged in the opendaylight package included in RHEL.
CVE-2018-10898	A vulnerability was found in openstack-tripleo-heat-templates before version 8.0.2-40. When deployed using Director using default configuration, Opendaylight in RHOSP13 is configured with easily guessable default credentials.
CVE-2018-1078	OpenDayLight version Carbon SR3 and earlier contain a vulnerability during node reconciliation that can result in traffic flows that should be expired or should expire shortly being re-installed and their timers reset resulting in traffic being allowed that should be expired.
CVE-2017-1000411	OpenFlow Plugin and OpenDayLight Controller versions Nitrogen, Carbon, Boron, Robert Varga, Anil Vishnoi contain a flaw when multiple 'expired' flows take up the memory resource of CONFIG DATASTORE which leads to CONTROLLER shutdown. If multiple different flows with 'idle-timeout' and 'hard-timeout' are sent to the Openflow Plugin REST API, the expired flows will eventually crash the controller once its resource allocations set with the JVM size are exceeded. Although the installed flows (with timeout set) are removed from network (and thus al controller's operations DS), the expired entries are still present in CONFIG DS. The attack can originate both from NORTH or SOUTH. The above description is for a north bound attack south bound attack can originate when an attacker attempts a flow flooding attack and since flows come with timeouts, the attack is not successful. However, the attacker will now be successful in CONTROLLER overflow attack (resource consumption). Although, the network (actual flow tables) and operational DS are only (~)1% occupied, the controller requests fo resource consumption. This happens because the installed flows get removed from the network upon timeout.
CVE-2017-1000406	OpenDaylight Karaf 0.6.1-Carbon fails to clear the cache after a password change, allowing the old password to be used until the Karaf cache is manually cleared (e.g. via restart).
CVE-2017-1000361	DOMRpcImplementationNotAvailableException when sending Port-Status packets to OpenDaylight. Controller launches exceptions and consumes more CPU resources. Component: OpenDaylight is vulnerable to this flaw. Version: The tested versions are OpenDaylight 3.3 and 4.0.
CVE-2017-1000360	StreamCorruptedException and NullPointerException in OpenDaylight odl-mdsal-xsql. Controller launches exceptions in the console. Component: OpenDaylight odl-mdsal-xsql is vulne this flaw. Version: The tested versions are OpenDaylight 3.3 and 4.0.
CVE-2017-1000359	Java out of memory error and significant increase in resource consumption. Component: OpenDaylight odl-mdsal-xsql is vulnerable to this flaw. Version: The tested versions are Open 3.3 and 4.0.
CVE-2017-1000358	Controller throws an exception and does not allow user to add subsequent flow for a particular switch. Component: OpenDaylight odl-restconf feature contains this flaw. Version: OpenDaylight 4.0 is affected by this flaw.
CVE-2017-1000357	Denial of Service attack when the switch rejects to receive packets from the controller. Component: This vulnerability affects OpenDaylight odl-l2switch-switch, which is the feature responsible for the OpenFlow communication. Version: OpenDaylight versions 3.3 (Lithium-SR3), 3.4 (Lithium-SR4), 4.0 (Beryllium), 4.1 (Beryllium-SR1), 4.2 (Beryllium-SR2), and 4. (Beryllium-SR4) are affected by this flaw. Java version is openjdk version 1.8.0_91.
CVE-2015-1857	The odl-mdsal-apidocs feature in OpenDaylight Helium allow remote attackers to obtain sensitive information by leveraging missing AAA restrictions.
CVE-2015-1778	The custom authentication realm used by karaf-tomcat's "opendaylight" realm in Opendaylight before Helium SR3 will authenticate any username and password combination.
CVE-2015-1612	OpenFlow plugin for OpenDaylight before Helium SR3 allows remote attackers to spoof the SDN topology and affect the flow of data, related to the reuse of LLDP packets, aka "LLDP Relay."
CVE-2015-1611	OpenFlow plugin for OpenDaylight before Helium SR3 allows remote attackers to spoof the SDN topology and affect the flow of data, related to "fake LLDP injection."
CVE-2015-1610	hosttracker in OpenDaylight l2switch allows remote attackers to change the host location information by spoofing the MAC address, aka "topology spoofing."
CVE-2014-8149	OpenDaylight defense4all 1.1.0 and earlier allows remote authenticated users to write report data to arbitrary files.
CVE-2014-5035	The Netconf (TCP) service in OpenDaylight 1.0 allows remote attackers to read arbitrary files via an XML external entity declaration in conjunction with an entity reference in an XML-RPC message, related to an XML External Entity (XXE) issue.

2014 – 2 CVEs
2015 – 5(4) CVEs
2016 – (2) CVEs
2017 – 8 CVEs
2018 – 2 CVEs

Security-specific Projects/Applications - ONOS

2015/2016
Security-Mode ONOS
Access Control based on DHCP
Access Control List (ACL)
AAA

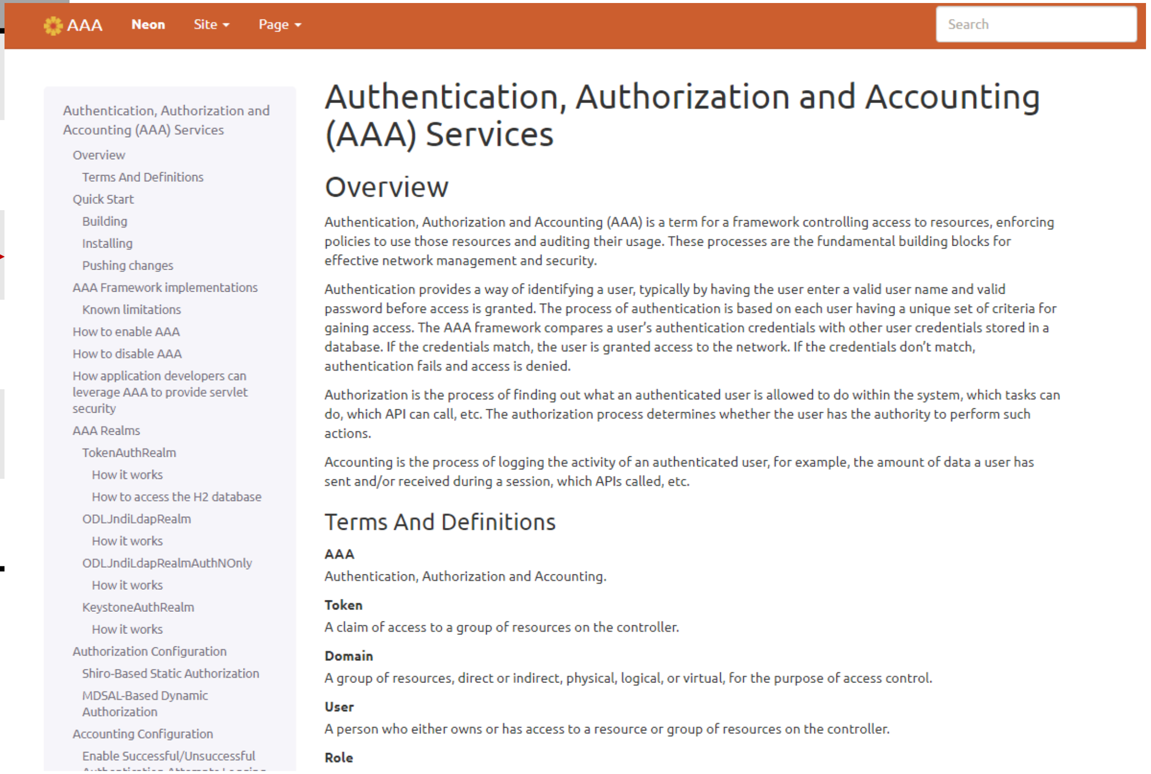
2017-2019
ARTEMIS (Automated System against BGP Prefix Hijacking)
VPLS (Virtual Private LAN Service)
Policy Framework for ONOS

Secure Controller Design
Control Process (Application) Isolation
Implementation of Policy Conflict Resolution
Multiple Controller Instances – Resilience
Multiple Application Instances – Resilience
Secure Storage

Security-specific Projects/Applications - ODL

2013-2016
Defense4All
Secure Network Bootstrapping Interface
AAA
Unified Secure Channel
Controller Shield
Cardinal – ODL Monitoring as a Service

Managed Project



- Authentication, Authorization and Accounting (AAA) Services
  - Overview
    - Terms And Definitions
  - Quick Start
    - Building
    - Installing
    - Pushing changes
  - AAA Framework implementations
    - Known limitations
  - How to enable AAA
  - How to disable AAA
  - How application developers can leverage AAA to provide servlet security
  - AAA Realms
    - TokenAuthRealm
      - How it works
      - How to access the H2 database
    - ODLJndiLdapRealm
      - How it works
    - ODLJndiLdapRealmAuthNOnly
      - How it works
    - KeystoneAuthRealm
      - How it works
  - Authorization Configuration
    - Shiro-Based Static Authorization
    - MDSAL-Based Dynamic Authorization
  - Accounting Configuration
    - Enable Successful/Unsuccessful

Authentication, Authorization and Accounting (AAA) Services

Overview

Authentication, Authorization and Accounting (AAA) is a term for a framework controlling access to resources, enforcing policies to use those resources and auditing their usage. These processes are the fundamental building blocks for effective network management and security.

Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA framework compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials don't match, authentication fails and access is denied.

Authorization is the process of finding out what an authenticated user is allowed to do within the system, which tasks can do, which API can call, etc. The authorization process determines whether the user has the authority to perform such actions.

Accounting is the process of logging the activity of an authenticated user, for example, the amount of data a user has sent and/or received during a session, which APIs called, etc.

Terms And Definitions

AAA

Authentication, Authorization and Accounting.

Token

A claim of access to a group of resources on the controller.

Domain

A group of resources, direct or indirect, physical, logical, or virtual, for the purpose of access control.

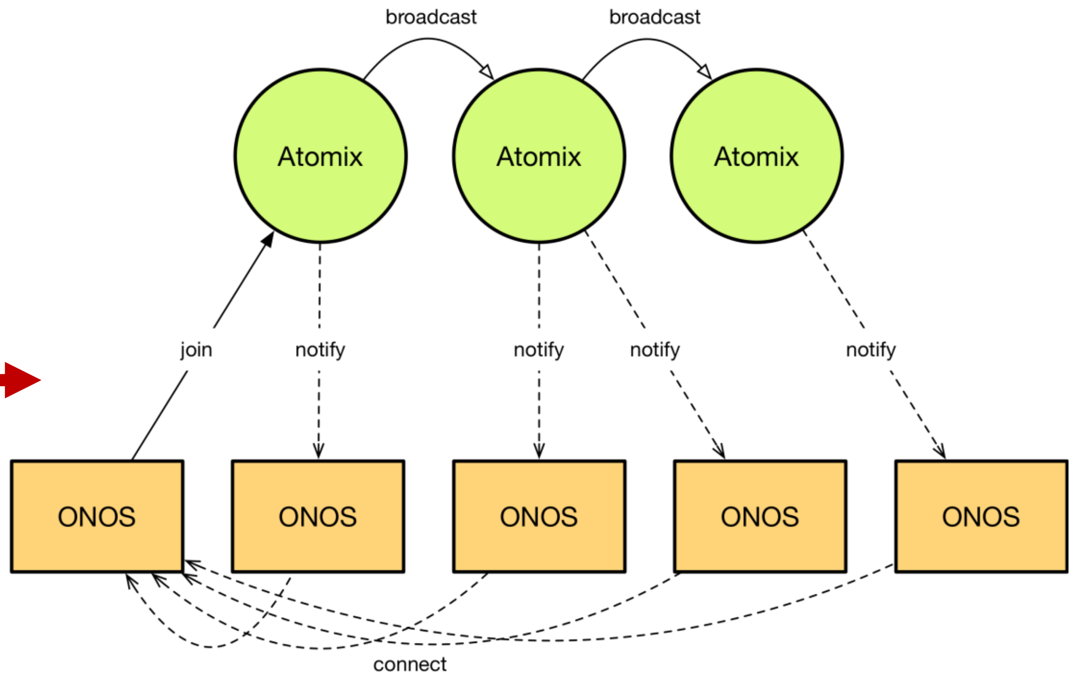
User

A person who either owns or has access to a resource or group of resources on the controller.

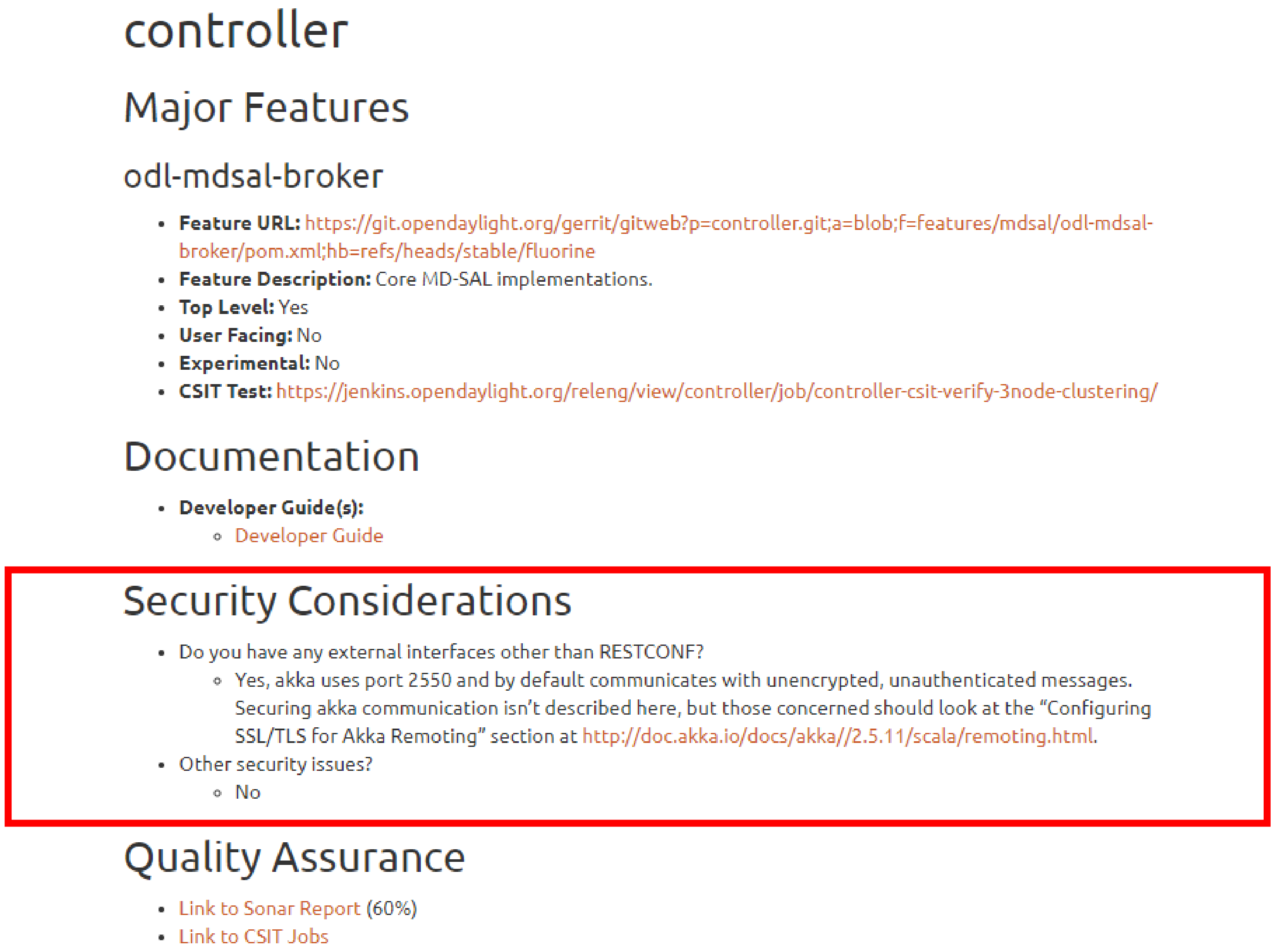
Role

Security-focused design - ONOS

Secure Controller Design
Control Process (Application) Isolation
Implementation of Policy Conflict Resolution
Multiple Controller Instances – Resilience
Multiple Application Instances – Resilience
Secure Storage



Security-focused design - ODL



controller

Major Features

odl-mdsal-broker

- **Feature URL:** https://git.opendaylight.org/gerrit/gitweb?p=controller.git;a=blob;f=features/mdsal/odl-mdsal-broker/pom.xml;hb=refs/heads/stable/fluorine
- **Feature Description:** Core MD-SAL implementations.
- **Top Level:** Yes
- **User Facing:** No
- **Experimental:** No
- **CSIT Test:** https://jenkins.opendaylight.org/releng/view/controller/job/controller-csit-verify-3node-clustering/

Documentation

- **Developer Guide(s):**
  - Developer Guide

Security Considerations

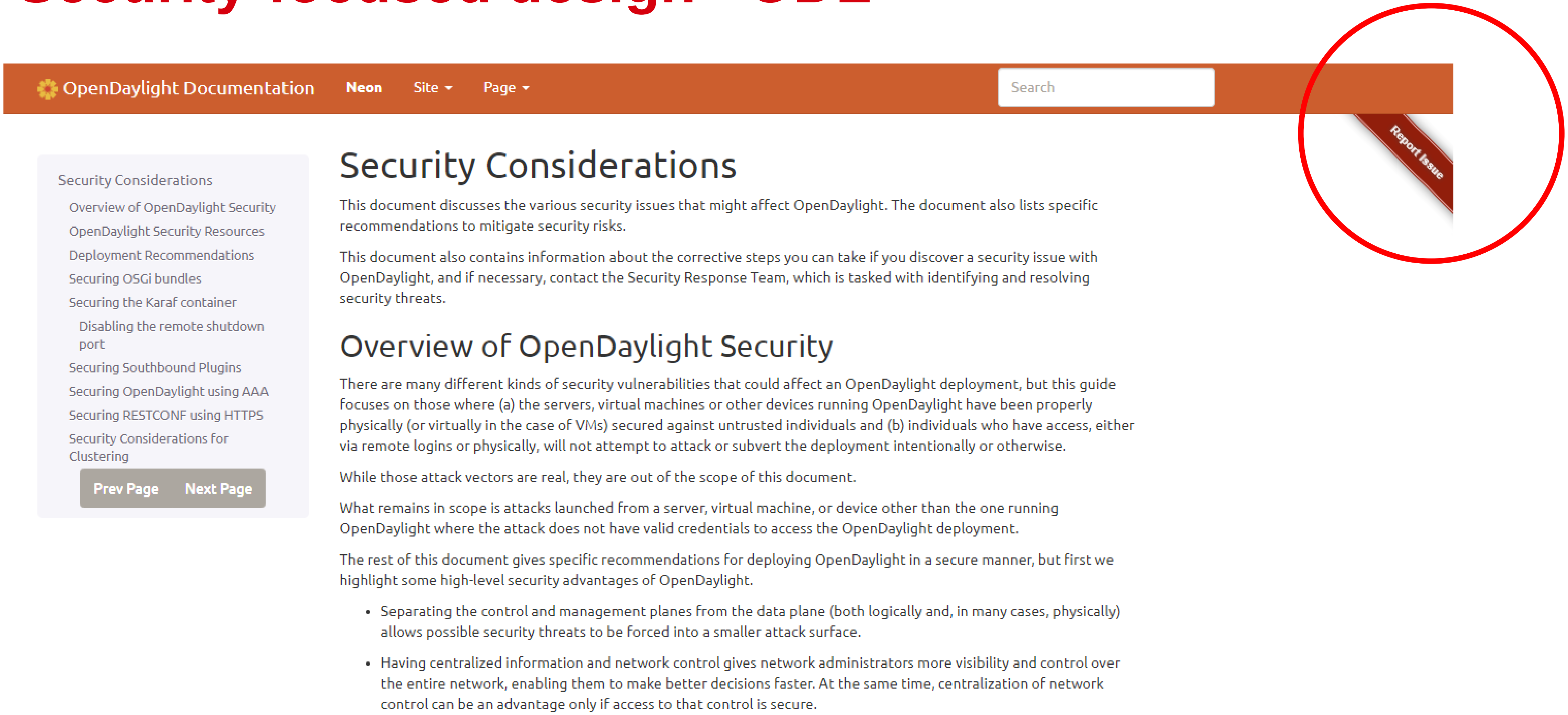
- Do you have any external interfaces other than RESTCONF?
  - Yes, akka uses port 2550 and by default communicates with unencrypted, unauthenticated messages. Securing akka communication isn't described here, but those concerned should look at the "Configuring SSL/TLS for Akka Remoting" section at http://doc.akka.io/docs/akka//2.5.11/scala/remoting.html.
- Other security issues?
  - No

Quality Assurance

- Link to Sonar Report (60%)
- Link to CSIT Jobs

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Security-focused design - ODL


OpenDaylight Documentation
Neon
Site
Page
Search
Report Issue
Security Considerations
Overview of OpenDaylight Security
OpenDaylight Security Resources
Deployment Recommendations
Securing OSGi bundles
Securing the Karaf container
Disabling the remote shutdown port
Securing Southbound Plugins
Securing OpenDaylight using AAA
Securing RESTCONF using HTTPS
Security Considerations for Clustering
Prev Page
Next Page

Security Considerations

This document discusses the various security issues that might affect OpenDaylight. The document also lists specific recommendations to mitigate security risks.

This document also contains information about the corrective steps you can take if you discover a security issue with OpenDaylight, and if necessary, contact the Security Response Team, which is tasked with identifying and resolving security threats.

Overview of OpenDaylight Security

There are many different kinds of security vulnerabilities that could affect an OpenDaylight deployment, but this guide focuses on those where (a) the servers, virtual machines or other devices running OpenDaylight have been properly physically (or virtually in the case of VMs) secured against untrusted individuals and (b) individuals who have access, either via remote logins or physically, will not attempt to attack or subvert the deployment intentionally or otherwise.

While those attack vectors are real, they are out of the scope of this document.

What remains in scope is attacks launched from a server, virtual machine, or device other than the one running OpenDaylight where the attack does not have valid credentials to access the OpenDaylight deployment.

The rest of this document gives specific recommendations for deploying OpenDaylight in a secure manner, but first we highlight some high-level security advantages of OpenDaylight.

- Separating the control and management planes from the data plane (both logically and, in many cases, physically) allows possible security threats to be forced into a smaller attack surface.
- Having centralized information and network control gives network administrators more visibility and control over the entire network, enabling them to make better decisions faster. At the same time, centralization of network control can be an advantage only if access to that control is secure.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Conclusion

OpenDaylight

ONOS

Meanwhile … *"Tungsten Fabric* (formerly known as *OpenContrail*) is a secure software defined networking project designed for the cloud native, multicloud environment."

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

References/Links

[1] Scott-Hayward, Sandra. "Trailing the Snail: SDN Controller Security Evolution." *arXiv preprint arXiv:1711.08406* (2017).

[2] OpenDaylight Vulnerability Management Process [Online] Available:
https://wiki.opendaylight.org/view/Security:Vulnerability_Management#Risk_Assessment

[3] ONOS CVE list [Online] Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ONOS

[4] ODL CVE list [Online] Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=OpenDaylight

[5] “Security-Mode ONOS.” [Online]. Available: https://wiki.onosproject.org/display/ONOS/Security-Mode+ONOS

[6] “Access Control Based on DHCP.” [Online]. Available:
https://wiki.onosproject.org/display/ONOS/Access+Control+Based+on+DHCP

[7] “ARTEMIS: an Automated System against BGP Prefix Hijacking.” [Online]. Available:
https://wiki.onosproject.org/display/ONOS/ARTEMIS%3A+an+Automated+System+against+BGP+Prefix+Hijacking

[8] “Virtual Private LAN Service - VPLS” [Online] Available:
https://wiki.onosproject.org/display/ONOS/Virtual+Private+LAN+Service+-+VPLS

[9] “Policy framework for ONOS” [Online] Available:
https://wiki.onosproject.org/display/ONOS/POLICY+FRAMEWORK+FOR+ONOS

[10] Scott-Hayward, Sandra. "Design and deployment of secure, robust, and resilient SDN Controllers." In *Proceedings of the 2015 1st IEEE conference on network Softwarization (NetSoft)*, pp. 1-5. IEEE, 2015.

[11] “Authentication, Authorization, and Accounting (AAA) Services” [Online] Available:
https://docs.opendaylight.org/projects/aaa/en/latest/dev-guide.html

[12] “Cluster Configuration in Owl (1.14)” [Online] Available:
https://wiki.onosproject.org/pages/viewpage.action?pageId=28836788

Thank you

s.scott-hayward@qub.ac.uk

www.csit.qub.ac.uk

CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES