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
Centre for Secure Information Technologies (CSIT)

CSIT is the UK’s Innovation and Knowledge Centre for Cybersecurity
SDNFV Security Research - Objectives

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

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

Security

Created by David Jorm, last modified by Thomas Vachuska on Mar 28, 2013

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, please detail 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 Pieterse

Security advisories

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

Back to security advisories main page.
## Security Support - ONOS

### CVE List

There are 12 CVE entries that match your search.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Year</th>
<th>CVEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-1099020</td>
<td>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.</td>
<td>2018</td>
<td>5</td>
</tr>
<tr>
<td>CVE-2018-12691</td>
<td>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.</td>
<td>2018</td>
<td>5</td>
</tr>
<tr>
<td>CVE-2018-1000616</td>
<td>ONOS ONOS controller version 1.13.1 and earlier contains an 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.</td>
<td>2018</td>
<td>5</td>
</tr>
<tr>
<td>CVE-2018-1000615</td>
<td>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.</td>
<td>2018</td>
<td>5</td>
</tr>
<tr>
<td>CVE-2018-1000614</td>
<td>ONOS ONOS Controller version 1.13.1 and earlier contains an XML External Entity (XXE) vulnerability in providers/netconf/alarms/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.</td>
<td>2018</td>
<td>5</td>
</tr>
<tr>
<td>CVE-2017-13753</td>
<td>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.</td>
<td>2017</td>
<td>6</td>
</tr>
<tr>
<td>CVE-2017-13752</td>
<td>ONOS versions 1.8.0, 1.9.0, and 1.10.0 are vulnerable to XSS.</td>
<td>2017</td>
<td>6</td>
</tr>
<tr>
<td>CVE-2017-1000681</td>
<td>Linux foundation ONOS 1.9.0 is vulnerable to unauthenticated upload of applications (.oar) resulting in remote code execution.</td>
<td>2017</td>
<td>6</td>
</tr>
<tr>
<td>CVE-2017-1000680</td>
<td>Linux foundation ONOS 1.9.0 allows unauthenticated use of websockets.</td>
<td>2017</td>
<td>6</td>
</tr>
<tr>
<td>CVE-2017-1000679</td>
<td>Linux foundation ONOS 1.9.0 is vulnerable to a DoS.</td>
<td>2017</td>
<td>6</td>
</tr>
<tr>
<td>CVE-2017-1000678</td>
<td>Linux foundation ONOS 1.9 is vulnerable to XSS in the device, registration.</td>
<td>2017</td>
<td>6</td>
</tr>
<tr>
<td>CVE-2015-7516</td>
<td>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).</td>
<td>2015</td>
<td>1</td>
</tr>
</tbody>
</table>

**Total CVE Entries:** 116825

2015 – 1 CVE
2017 – 6 CVEs
2018 – 5 CVEs
Security Support - ODL

Security: Vulnerability Management

Contents

- OpenDaylight - Vulnerability Management
  - 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
      - 1.3.3.6 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

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 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 Selfried
- Ryan Goudling
- Lori Jakab
- Stephen Kitt

Security advisories

The security advisories page lists all security vulnerabilities fixed in OpenDaylight.
Security Support - ODL

2014 – 2 CVEs
2015 – 5(4) CVEs
2016 – (2) CVEs
2017 – 8 CVEs
2018 – 2 CVEs
Security-specific Projects/Applications - ONOS

<table>
<thead>
<tr>
<th>2015/2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security-Mode ONOS</td>
</tr>
<tr>
<td>Access Control based on DHCP</td>
</tr>
<tr>
<td>Access Control List (ACL)</td>
</tr>
<tr>
<td>AAA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2017-2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARTEMIS (Automated System against BGP Prefix Hijacking)</td>
</tr>
<tr>
<td>VPLS (Virtual Private LAN Service)</td>
</tr>
<tr>
<td><strong>Policy Framework for ONOS</strong></td>
</tr>
</tbody>
</table>

**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
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=bltj;f=features/mdsal/odl-mdsal-broker/pom.xml;h=brefs/heads/stable/fluorine
- Feature Description: Core IIM-SAL Implementations.
- Top Level: Yes
- User Facing: No
- Experimental: No
- CSIT Test: https://jenkins.opendaylight.org/relegen/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
Security-focused design - ODL

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 login or physically, will not attempt to attack or subvert the deployment intentionally or otherwise.

While these 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.
Conclusion

Meanwhile ... “Tungsten Fabric (formerly known as OpenContrail) is a secure software defined networking project designed for the cloud native, multicloud environment.”
References/Links

Thank you

s.scott-hayward@qub.ac.uk
www.csit.qub.ac.uk