ONOS Security
Recent Vulnerabilities & Fixes

Dylan Smyth
17-06-2019
$whoami

- PhD Student (Almost finished!)

- Security in Software-Defined Networks
  - Exploiting pitfalls in software-defined networking implementation
  - Detecting link fabrication attacks in software-defined networks
  - Attacking Distributed Software-Defined Networks By Leveraging Network State Consistency

- Involved with ONOS SecPerf brigade since April 2017
ONOS Security

- Past
  - Vulnerabilities prior to 2018

- Present
  - 2018 & 2019

- Future
  - Where might more bugs be hiding?
ONOS Security: Past

- Denial of Service
  - CVE-2015-1166 - ONOS disconnects switch after receiving malformed packet (of-ctl)
  - CVE-2015-7516 - ONOS disconnects switch after receiving malformed packet (app proc.)
  - CVE-2015-7516 - IPFW app jumbo ethernet frame
  - CVE-2017-13763 - Memory leak in clustering caused by malformed message
  - CVE-2017-1000079 - Long strings sent to restconf causes incorrect operation
ONOS Security: Past

- Denial of Service
  - CVE-2015-1166 - ONOS disconnects switch after receiving malformed packet (of-ctl)
  - CVE-2015-7516 - ONOS disconnects switch after receiving malformed packet (app proc.)
  - CVE-2015-7516 - IPFW app jumbo ethernet frame
  - CVE-2017-13763 - Memory leak in clustering caused by malformed message
  - CVE-2017-1000079 - Long strings sent to restconf causes incorrect operation
ONOS Security: Past

- Web Application
  - CVE-2017-13763 - XSS via switch details provided through the southbound interface
  - CVE-2017-1000078 - XSS via switch details provided through restconf
  - CVE-2017-1000080 - Unauthenticated websocket usage
  - CVE-2017-1000081 - Unauthenticated application upload
ONOS Security: Past

- **Web Application**
  - CVE-2017-13763 - XSS via `switch details` provided through the southbound interface
  - CVE-2017-1000078 - XSS via `switch details` provided through restconf
  - CVE-2017-1000080 - Unauthenticated websocket usage
  - CVE-2017-1000081 - Unauthenticated application upload
ONOS Security: Past

- Web Application
  - CVE-2017-13763 - XSS via switch details provided through the southbound interface
  - CVE-2017-1000078 - XSS via switch details provided through restconf
  - CVE-2017-1000080 - Unauthenticated websocket usage
  - CVE-2017-1000081 - Unauthenticated application upload
ONOS Security: Present

- **XML External Entity (XXE)**
  - CVE-2018-1000614 - XXE in Netconf Alarm Translator
  - CVE-2018-1000616 - XXE in XML Config Parser

- **Denial of Service**
  - CVE-2018-1000615 - OVSDB service crash via switch version formatting

- **Bypass**
  - CVE-2018-12691 - Time-of-Use race condition leads to ACL bypass, invalid packet can corrupt HIB and prevent ACL rule installation
ONOS Security: Present

- XML External Entity (XXE)
  - CVE-2018-1000614 - XXE in Netconf Alarm Translator
  - CVE-2018-1000616 - XXE in XML Config Parser

- Denial of Service
  - CVE-2018-1000615 - OVSDB service crash via `switch version formatting`

- Bypass
  - CVE-2018-12691 - Time-of-Use race condition leads to ACL bypass, `invalid packet` can corrupt HIB and prevent ACL rule installation
- Link Fabrication Attack defence implemented

- LLDP frames now include a Message Authentication Code

- LLDP frames also include a timestamp, and should not be more than 1 second old when received.
Vulnerabilities can often cluster
ONOS Security: Future

- Vulnerabilities can often cluster
- ONOS offers many features
Vulnerabilities can often cluster

ONOS offers many features (Lots of complex code!)
Vulnerabilities can often cluster

ONOS offers many features (Lots of complex code!)

Where should we look?
  - Clustering, southbound drivers <- Where information may be assumed to be correct
  - Restconf <- User supplied data may not be checked
Thank you