

# HPE Software Security Update

## HPE Propel Update for V8 (DoS) Buffer Overflow (CVE-2016-1669)

---

### Document management:

Date	Version	Change
6-Sep-2016	1.0	Initial Release
12-Oct-2016	1.1	Update with offline instructions.

### Summary:

Under certain conditions, V8 may improperly expand memory allocations in the `Zone::New` function. This could potentially be used to cause a Denial of Service via buffer overflow or as a trigger for a remote code execution.

Read more about how Node.js is affected by CVE-2016-1669 in their [June blog entry](#).

### Topic

Find out more about CVE-2016-1669 from the [MITRE CVE dictionary](#) dictionary and [NIST NVD](#).

*HPE has investigated the CVE-2016-1669 vulnerability in relation to HPE Propel. This document provides required actions that must be performed to mitigate these vulnerabilities.*

**Affected Releases: 1.01, 1.11, 2.01, 2.10, 2.20**

**ACTION:** Review all details in instructions provided in this paper to address the vulnerability. HPE SW recommend to address this information as soon as possible.

## Response

## Impact on HPE Propel

The 1.01, 1.11, 2.01, 2.10 and 2.20 versions of the HPE Propel OVA (Virtual Appliance) ship with older versions of Node.js which are vulnerable to CVE-2016-1669. The Node.js version can be determined by executing the command

```
# node -v
```

## Mitigation Actions

Update Node.js to the latest stable release:

```
# curl -sL https://rpm.nodesource.com/setup_4.x | bash -  
# yum -y install nodejs npm
```

If you do not have Internet access, obtain the RPM from:

```
https://rpm.nodesource.com/pub\_4.x/e1/7/x86\_64/nodejs-4.5.0-1nodesource.e17.centos.x86\_64.rpm
```

Copy the RPM to the /tmp directory on the HPE Propel VM. Remove NodeJS from the HPE Propel VM:

```
# yum remove nodejs
```

Manually install the new rpm from the the /tmp directory on the HPE Propel VM:

```
# rpm -ivh /tmp/nodejs-4.5.0-1nodesource.e17.centos.x86_64.rpm
```

After mitigation, 'node -v' should report v4.4.6 or newer.

## HPE Propel Update for V8 (DoS) Buffer Overflow (CVE-2016-1669)

©Copyright 2015 Hewlett-Packard Enterprise Development Company, L.P.

Hewlett-Packard Enterprise Company shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HPE or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett-Packard Company and the names of Hewlett-Packard Enterprise products referenced herein are trademarks of Hewlett-Packard Enterprise Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.