

# Advisory Alert

Alert No: AAA181018

Date: 18-Oct-18 12:09 PM



## Security Updates for 18<sup>th</sup> October 2018

<b>Overview</b>	<table> <tr> <td rowspan="4" style="vertical-align: middle; text-align: center;"><b>High</b></td> <td>libssh</td> <td>▪ Bypass Security Restrictions</td> </tr> <tr> <td>Oracle</td> <td>▪ Multiple Vulnerabilities</td> </tr> <tr> <td>Drupal</td> <td>▪ Multiple Vulnerabilities</td> </tr> <tr> <td>Cisco</td> <td>▪ Multiple Vulnerabilities</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td style="vertical-align: middle; text-align: center;"><b>Medium</b></td> <td>WebSphere</td> <td>▪ Cross-Site Scripting Attack</td> </tr> </table>	<b>High</b>	libssh	▪ Bypass Security Restrictions	Oracle	▪ Multiple Vulnerabilities	Drupal	▪ Multiple Vulnerabilities	Cisco	▪ Multiple Vulnerabilities	<hr/>			<b>Medium</b>	WebSphere	▪ Cross-Site Scripting Attack
<b>High</b>	libssh		▪ Bypass Security Restrictions													
	Oracle		▪ Multiple Vulnerabilities													
	Drupal		▪ Multiple Vulnerabilities													
	Cisco	▪ Multiple Vulnerabilities														
<hr/>																
<b>Medium</b>	WebSphere	▪ Cross-Site Scripting Attack														
<b>Description / Impact</b>	<table> <tr> <td style="vertical-align: top;"><b>libssh</b></td> <td> <ul style="list-style-type: none"> <li>A vulnerability in libssh could allow a remote attacker to bypass security restrictions.</li> <li>Affected Products: <b>libssh 0.6.0, 0.7.5, 0.8.3</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> </td> </tr> <tr> <td style="vertical-align: top;"><b>Oracle</b></td> <td> <ul style="list-style-type: none"> <li>Oracle has released the October 2018 patch update</li> <li>Affected Products: <b>MySQL Server, Oracle Database Server, Oracle Java SE, Solaris, Java ME, Fusion Middleware, E-Business suit, Financial Services Applications, Virtualization</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> </td> </tr> <tr> <td style="vertical-align: top;"><b>Drupal</b></td> <td> <ul style="list-style-type: none"> <li>Drupal has released updates to address multiple vulnerabilities affecting Drupal products.</li> <li>Affected Products: <b>Drupal 7.0, 8.0</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> </td> </tr> <tr> <td style="vertical-align: top;"><b>Cisco</b></td> <td> <ul style="list-style-type: none"> <li>Cisco has released updates to address multiple vulnerabilities affecting Cisco products.</li> <li>Affected Products: <b>Cisco Nexus 5500 Series Switches Cisco Nexus 5600 Series Switches Cisco Nexus 6000 Series Switches - Standalone, NX-OS mode And other multiple products</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> </td> </tr> <tr> <td style="vertical-align: top;"><b>WebSphere</b></td> <td> <ul style="list-style-type: none"> <li>A vulnerability IBM WebSphere Application Server could allow users to embed arbitrary JavaScript code in the Web UI.</li> <li>Affected Products:</li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> </td> </tr> </table>	<b>libssh</b>	<ul style="list-style-type: none"> <li>A vulnerability in libssh could allow a remote attacker to bypass security restrictions.</li> <li>Affected Products: <b>libssh 0.6.0, 0.7.5, 0.8.3</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>	<b>Oracle</b>	<ul style="list-style-type: none"> <li>Oracle has released the October 2018 patch update</li> <li>Affected Products: <b>MySQL Server, Oracle Database Server, Oracle Java SE, Solaris, Java ME, Fusion Middleware, E-Business suit, Financial Services Applications, Virtualization</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>	<b>Drupal</b>	<ul style="list-style-type: none"> <li>Drupal has released updates to address multiple vulnerabilities affecting Drupal products.</li> <li>Affected Products: <b>Drupal 7.0, 8.0</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>	<b>Cisco</b>	<ul style="list-style-type: none"> <li>Cisco has released updates to address multiple vulnerabilities affecting Cisco products.</li> <li>Affected Products: <b>Cisco Nexus 5500 Series Switches Cisco Nexus 5600 Series Switches Cisco Nexus 6000 Series Switches - Standalone, NX-OS mode And other multiple products</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>	<b>WebSphere</b>	<ul style="list-style-type: none"> <li>A vulnerability IBM WebSphere Application Server could allow users to embed arbitrary JavaScript code in the Web UI.</li> <li>Affected Products:</li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>					
<b>libssh</b>	<ul style="list-style-type: none"> <li>A vulnerability in libssh could allow a remote attacker to bypass security restrictions.</li> <li>Affected Products: <b>libssh 0.6.0, 0.7.5, 0.8.3</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>															
<b>Oracle</b>	<ul style="list-style-type: none"> <li>Oracle has released the October 2018 patch update</li> <li>Affected Products: <b>MySQL Server, Oracle Database Server, Oracle Java SE, Solaris, Java ME, Fusion Middleware, E-Business suit, Financial Services Applications, Virtualization</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>															
<b>Drupal</b>	<ul style="list-style-type: none"> <li>Drupal has released updates to address multiple vulnerabilities affecting Drupal products.</li> <li>Affected Products: <b>Drupal 7.0, 8.0</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>															
<b>Cisco</b>	<ul style="list-style-type: none"> <li>Cisco has released updates to address multiple vulnerabilities affecting Cisco products.</li> <li>Affected Products: <b>Cisco Nexus 5500 Series Switches Cisco Nexus 5600 Series Switches Cisco Nexus 6000 Series Switches - Standalone, NX-OS mode And other multiple products</b></li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>															
<b>WebSphere</b>	<ul style="list-style-type: none"> <li>A vulnerability IBM WebSphere Application Server could allow users to embed arbitrary JavaScript code in the Web UI.</li> <li>Affected Products:</li> <li>Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul>															
<b>Risk Reduction Recommendations</b>	<p>Visit the links below and follow the instructions given by respective vendors.</p> <table> <tr> <td>libssh</td> <td><a href="https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/">https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/</a></td> </tr> <tr> <td>Oracle</td> <td><a href="https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html">https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html</a></td> </tr> <tr> <td>Drupal</td> <td><a href="https://www.drupal.org/sa-core-2018-006">https://www.drupal.org/sa-core-2018-006</a></td> </tr> <tr> <td>Cisco</td> <td><a href="https://tools.cisco.com/security/center/publicationListing.x">https://tools.cisco.com/security/center/publicationListing.x</a></td> </tr> <tr> <td>WebSphere</td> <td><a href="https://www-01.ibm.com/support/docview.wss?uid=ibm10730631">https://www-01.ibm.com/support/docview.wss?uid=ibm10730631</a></td> </tr> </table>	libssh	<a href="https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/">https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/</a>	Oracle	<a href="https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html">https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html</a>	Drupal	<a href="https://www.drupal.org/sa-core-2018-006">https://www.drupal.org/sa-core-2018-006</a>	Cisco	<a href="https://tools.cisco.com/security/center/publicationListing.x">https://tools.cisco.com/security/center/publicationListing.x</a>	WebSphere	<a href="https://www-01.ibm.com/support/docview.wss?uid=ibm10730631">https://www-01.ibm.com/support/docview.wss?uid=ibm10730631</a>					
libssh	<a href="https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/">https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/</a>															
Oracle	<a href="https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html">https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html</a>															
Drupal	<a href="https://www.drupal.org/sa-core-2018-006">https://www.drupal.org/sa-core-2018-006</a>															
Cisco	<a href="https://tools.cisco.com/security/center/publicationListing.x">https://tools.cisco.com/security/center/publicationListing.x</a>															
WebSphere	<a href="https://www-01.ibm.com/support/docview.wss?uid=ibm10730631">https://www-01.ibm.com/support/docview.wss?uid=ibm10730631</a>															
<b>Disclaimer</b>	<p>The information provided herein is on "as is" basis, without warranty of any kind.</p>															