WSO2 Security Vulnerability Management Process

Version: 1.6 | Date: 17th Mar 2020

WSO2 conducts security reviews and tests throughout the entire software development lifecycle (SDLC) to make sure our products and services are secure against all known vulnerabilities. However, even with the most stringent tests, some vulnerabilities can go unnoticed. That is why WSO2 treats security vulnerability disclosures with the highest priority. We have an efficient process to evaluate such disclosures urgently and take steps to mitigate risks.

This document explains the processes used to handle security vulnerabilities from their discovery to mitigation:

- Security Vulnerability Sources
- Severity Classification
- Resolution Timeframes
- Vulnerability Handling Process
- Backporting Policy
- Announcing to the Customers
- Announcing to the Public
- Providing Acknowledgements

Security Vulnerability Sources

We receive security vulnerability information mainly via the following sources:

- Internal security tests and scans:
  We conduct security scanning using multiple industry standard products and tools on released WSO2 product versions as well as versions under development.

- The security@wso2.com mailing list:
  Any user who comes across security issues in WSO2 products and services is highly encouraged to report those issues via this channel.

- Customer Support Portal:
  Users with a paid WSO2 subscription can report security issues via this channel.

Before reporting a vulnerability to WSO2, make sure you follow the recommendations given in WSO2 Security Vulnerability Reporting Guidelines.

Please note that we highly discourage sending automated scan reports via security@wso2.com. The WSO2 Platform Security team does not put effort to evaluate such scan reports due to the high percentage of false positives that are inherent in automated security scanning. Therefore, please report positive vulnerabilities with steps to reproduce as explained in WSO2 Security Vulnerability Reporting Guidelines.

Severity Classification

We follow the Common Vulnerability Scoring System v3.0 to rate the vulnerabilities that are reported to us.

Given below is the WSO2 severity classification, and how it maps to the CVSS 3.0 scoring system:

<table>
<thead>
<tr>
<th>Classification</th>
<th>CVSS Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>9.0 - 10.0</td>
</tr>
</tbody>
</table>
Resolution Timeframes

Given below are two examples of how timeframes are calculated:

1. A customer reports vulnerabilities found by an automated scan or a manual pen-test. In this case, the resolution timeframes change based on the severity of the vulnerability. WSO2 calculates these timeframes from the date that the vulnerability has been confirmed as a True Positive. For example:

<table>
<thead>
<tr>
<th>Classification</th>
<th>CVSS score</th>
<th>Resolution Time (up to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>9.0 - 10.0</td>
<td>7 days</td>
</tr>
<tr>
<td>High</td>
<td>7.0 - 8.9</td>
<td>14 days</td>
</tr>
<tr>
<td>Medium</td>
<td>4.0 - 6.9</td>
<td>30 days</td>
</tr>
<tr>
<td>Low</td>
<td>3.9 or below</td>
<td>Next product release, or at product team's discretion</td>
</tr>
</tbody>
</table>

Note that once a fix is given to this customer, if there are other customers using the same product version, they can also get the same fix by using WSO2 Update Manager (WUM). WSO2 informs about security fixes to customers via a monthly announcement mailer. However, if it's a vulnerability with catastrophic implications, the fix is immediate announced to all customers.

2. A customer reports a security breach. WSO2 takes immediate action irrespective of the severity of the vulnerability.

Vulnerability Handling Process

Given below is the process of handling a security vulnerability notification:

1. WSO2 team receives a notification about a security vulnerability, acknowledges it, and creates an internal ticket to track its progress.
2. The vulnerability is treated as highest priority and directed to the respective product or services team.
3. The product or services team evaluates the vulnerability with help from the security champion of the product and the Platform Security team.
4. If the vulnerability does not pose a threat to the product or service, WSO2 responds back with proper reasoning.
5. If the reported vulnerability is an actual threat, WSO2 responds back, accepting the issue.
6. The product team provides a quick solution, if available. (E.g., a configuration change to disable some functionality). If not, the product team works to identify a fix.
7. If the reporter is a WSO2 customer, give a time estimation (ETA) to create the patch for a particular product version.
8. If the reporter is not a WSO2 customer, WSO2 does the following:
   a. Identify all the product versions that need to be fixed (See Back Porting Policy for more information).
   b. Estimate the effort to patch all of them.
   c. Come up with a date to issue the fixes to the customers.
   d. Add a 1-month buffer to come up with the public announcement date.
   e. According to the WSO2's responsible disclosure ethics, inform the public announcement date to the issue reporter first. If the reporter agrees to making the vulnerability information public, then the information will be announced after the previously set public announcement date.
9. Initiate the patch creation process.
10. Create an internal identifier for the issue in the format WSO2-<year>-<ticket number>. For example, WSO2-2016-0010.
11. Create a Security Advisory for the vulnerability, informing its impact and the mitigation steps.
12. If the reporter is a customer of WSO2, the patch/update is provided to the reporter.
13. If the reporter is not a customer of WSO2, upon request by the reporter, WSO2 provides the source code diff so that the reporter can understand the fix and apply it. A public security advisory will be issued after all the patches are issued to the customers and the buffer period is exceeded.

Backporting Policy

Backporting policy is to provide fixes upto 3 years or upon request by the customers who are using product versions that are older than 3 years and have a subscription with WSO2.

Backported fixes are available to the customers either through WSO2 Update Manager or the support channel (if the product version does not support WUM).

For the release dates of all WSO2 products, see the Release Matrix.

Announcing to the Customers

Once the fix for a particular true positive vulnerability is identified and the security advisories are created for all the affected product versions that are within the backporting policy, they need to be shared with all the WSO2 customers. This is done via a ‘Customer Announcement’ that happens on the last working day of the month. However, if the vulnerability was reported by a customer, then the fix is given to that particular customer without waiting until the monthly announcement.

Announcing to the Public

Once the customer announcement is done, we give a buffer period of 4 weeks for customers to apply the patches. After the buffer period, the vulnerability is publicly announced on the Security Advisories page. The contents of the public security advisory depends on several factors:

- If CVSS score of the issue is greater than or equal to 9.0 (CVSS ≥ 9), and the latest version of a WSO2 product is affected, a patch release of the particular product is done after all the patches are issued to the customers and the buffer period is exceeded. A public security advisory will be issued to inform about the issue and the availability of the patch release.
- If CVSS score of the issue is less than 9.0 (CVSS < 9), and the latest version of a WSO2 product is affected, a public security advisory will be issued after all the patches are issued to the customers and the buffer period is exceeded. The public security advisory will contain information about any available risk mitigations and the pull-request information of the fix (relevant changes to public source-code).
- If the latest version of any WSO2 product is not affected by the issue, public security advisory will be issued advising community users to update to the latest product version.

Providing Acknowledgements

WSO2 appreciates the efforts of security researchers to identify security vulnerabilities in our products. We give credits to such researchers in the relevant security advisories listed on the Security Advisories page and also include them in a dedicated Acknowledgments page. The inclusion to either page is done upon the researcher's consent.

For more information on the acknowledgement process, see WSO2 Security Reward and Acknowledgement Program.