



# Advisory Alert

Alert No: AAA20200522

Date: 22-May-20 11:00 AM

Classification

The Alert

: Public Circulation Permitted

## Security Updates for 22<sup>nd</sup> May 2020

|                               |  |  |   |
|-------------------------------|--|--|---|
| <b>Overview</b>               | <b>High</b>  | <b>Microsoft</b><br><b>PostgreSQL</b><br><b>Drupal</b> | <ul style="list-style-type: none"> <li>• Denial of Service Vulnerability</li> <li>• Privilege Escalation Vulnerability</li> <li>• Multiple Vulnerabilities</li> </ul> |
| <b>Description / Impact</b>   | <b>Microsoft</b> <ul style="list-style-type: none"> <li>• Microsoft has released a workaround that addresses the Vulnerability affecting Windows DNS Servers. An attacker could exploit this vulnerability to cause a denial-of-service condition.</li> <li>• Affected Products: <ul style="list-style-type: none"> <li>• <b>Windows DNS Servers</b></li> </ul> </li> <li>• Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> <hr/> <b>PostgreSQL</b> <ul style="list-style-type: none"> <li>• PostgreSQL has released security updates addressing a vulnerability in PostgreSQL installer for windows. Which an attacker could exploit this vulnerability to take control of an affected system.</li> <li>• Affected Products: <ul style="list-style-type: none"> <li>• <b>Windows installer Version 9.5 to 12</b></li> </ul> </li> <li>• Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> <hr/> <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: <ul style="list-style-type: none"> <li>• <b>Drupal 8.8 prior to 8.8.6</b></li> <li>• <b>Drupal 8.7 prior to 8.7.14</b></li> <li>• <b>Drupal 7 prior to 7.70</b></li> </ul> </li> <li>• Officially Acknowledged by the Vendor: <b>Yes</b></li> </ul> |  |   |
| <b>Additional Information</b> | Visit the links below and follow the instructions given by respective vendors according to your internal policies/ procedures.   |  |   |
|                               | <b>Microsoft</b> <ul style="list-style-type: none"> <li>• <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200009">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200009</a></li> </ul>   |  |   |
|                               | <b>PostgreSQL</b> <ul style="list-style-type: none"> <li>• <a href="https://www.postgresql.org/support/security/">https://www.postgresql.org/support/security/</a></li> </ul>  |  |   |
|                               | <b>Drupal</b> <ul style="list-style-type: none"> <li>• <a href="https://www.drupal.org/sa-core-2020-002">https://www.drupal.org/sa-core-2020-002</a></li> <li>• <a href="https://www.drupal.org/sa-core-2020-003">https://www.drupal.org/sa-core-2020-003</a></li> </ul>   |  |   |
| <b>Disclaimer</b>             | The information provided herein is on "as is" basis, without warranty of any kind.   |  |   |