Ambari Vulnerabilities

Fixed in Ambari 2.7.0

CVE-2018-8042: Passwords for Hadoop credential stores are visible in Ambari Agent standard out

Severity: Important

Vendor: Hortonworks

Versions Affected: Ambari 2.5.x, Ambari 2.6.x

Versions Fixed: Ambari 2.7.0

Description:
Passwords for Hadoop credential stores are exposed in Ambari Agent informational log messages when the credential store feature is enabled for eligible services. For example, Hive and Oozie.

Mitigation:
Ambari 2.5.x installations should be upgraded to Ambari 2.7.0
Ambari 2.6.x installations should be upgraded to Ambari 2.7.0

Credit:
This issue was discovered by Hortonworks.

Fixed in Ambari 2.6.2

CVE-2018-8003: Path traversal in Ambari allows remote and unauthenticated access to files in the filesystem

Severity: Important

Vendor: Hortonworks

Versions Affected: Ambari 1.4.0 through Ambari 2.6.1

Description: Ambari is susceptible to a directory traversal attack allowing an unauthenticated user to craft an HTTP request which provides read-only access to any file on the filesystem of the host the Ambari Server runs on that is accessible by the user the Ambari Server is running as. Direct network access to the Ambari Server is required to issue this request, and those Ambari Servers that are protected behind a firewall, or in a restricted network zone are at less risk of being affected by this issue.

Mitigation:
Ambari 2.5.x and earlier installations should be upgraded to Ambari 2.6.2
Ambari 2.6.0 installations should be upgraded to Ambari 2.6.2
Ambari 2.6.1 installations should be upgraded to Ambari 2.6.2

Credit: Krzysztof Przybylski from STM Solutions

Fixed in Ambari 2.5.1

CVE-2017-5654: XML injection vulnerability in Hive View

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.4.0 through 2.4.2, and 2.5.0

Versions Fixed: 2.4.3, 2.5.1

Description: An authorized user of the Ambari Hive View may be able to gain unauthorized read access to files on the host where the Amari server executes.
Access to files are limit to the set of files for which the user that executes the Ambari server has read access.

Mitigation: Ambari users should upgrade to version 2.4.3; or version 2.5.1 or above.

Credit: New York Life Insurance Company

CVE-2017-5655: Possible exposure of sensitive data in files created in Ambari temp directory when downloading configurations

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.2.2 through 2.4.2; and 2.5.0

Versions Fixed: 2.4.3, 2.5.1

Description: Sensitive data may be stored on disk in temporary files on the Ambari Server host. The temporary files are readable by any user authenticated on the host.

Mitigation: Ambari 2.4.x (before 2.4.3) users should upgrade to version 2.4.3; Ambari 2.5.0 users should upgrade to Ambari 2.5.1 or above.

Ambari 2.4.3 and Ambari 2.5.1 correct this issue by forcing the related temporary files to be accessible only to the user executing the Ambari server process. The related temporary files should be removed when no longer needed, as well.

Credit: Pradeep Bhadani

Fixed in Ambari 2.5.0

CVE-2017-5642: Ambari Server artifacts do not have proper ACLs

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.4.0 to 2.4.2

Versions Fixed: 2.4.3, 2.5.0

Description: During installation, Ambari Server artifacts are not created with proper ACLs

Mitigation: Ambari users should upgrade to version 2.5.0 or above. For users of Version 2.4.0 through Version 2.4.2, either upgrade to version 2.4.3 or execute the script provided with Version 2.5.0 to correct the ACLs on Ambari server artifacts.
The proper ACL's are set for installed Ambari artifacts in Ambari versions 2.4.3, 2.5.0 and later. However, users of Version 2.4.0 through 2.4.2 may execute the script found at https://github.com/apache/ambari/blob/release-2.5.0/ambari-server/src/main/resources/scripts/check_ambari_permissions.py to fix the permissions on Ambari server artifacts on the Ambari server host.

Credit: Hortonworks

Fixed in Ambari 2.4.3

CVE-2017-5642: Ambari Server artifacts do not have proper ACLs

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.4.0 to 2.4.2

Versions Fixed: 2.4.3, 2.5.0

Description: During installation, Ambari Server artifacts are not created with proper ACLs

Mitigation: Ambari users should upgrade to version 2.5.0 or above. For users of Version 2.4.0 through Version 2.4.2, either upgrade to version 2.4.3 or execute the script provided with Version 2.5.0 to correct the ACLs on Ambari server artifacts.
The proper ACL's are set for installed Ambari artifacts in Ambari versions 2.4.3, 2.5.0 and later. However, users of Version 2.4.0 through 2.4.2 may execute the script found at https://github.com/apache/ambari/blob/release-2.5.0/ambari-server/src/main/resources/scripts/check_ambari_permissions.py to fix the permissions on Ambari server artifacts on the Ambari server host.

Credit: Hortonworks

CVE-2017-5654: XML injection vulnerability in Hive View

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.4.0 through 2.4.2, and 2.5.0

Versions Fixed: 2.4.3, 2.5.1

Description: An authorized user of the Ambari Hive View may be able to gain unauthorized read access to files on the host where the Amari server executes.
Access to files are limit to the set of files for which the user that executes the Ambari server has read access.

Mitigation: Ambari users should upgrade to version 2.4.3; or version 2.5.1 or above.

Credit: New York Life Insurance Company

CVE-2017-5655: Possible exposure of sensitive data in files created in Ambari temp directory when downloading configurations

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.2.2 through 2.4.2; and 2.5.0

Versions Fixed: 2.4.3, 2.5.1

Description: Sensitive data may be stored on disk in temporary files on the Ambari Server host. The temporary files are readable by any user authenticated on the host.

Mitigation: Ambari 2.4.x (before 2.4.3) users should upgrade to version 2.4.3; Ambari 2.5.0 users should upgrade to Ambari 2.5.1 or above.

Ambari 2.4.3 and Ambari 2.5.1 correct this issue by forcing the related temporary files to be accessible only to the user executing the Ambari server process. The related temporary files should be removed when no longer needed, as well.

Credit: Pradeep Bhadani

Fixed in Ambari 2.4.2

CVE-2016-6807: Custom commands may be executed without authorization

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.4.0 to 2.4.1

Versions Fixed: 2.4.2

Description: Custom commands may be executed on the Ambari Agent hosts without authorization, leading to unauthorized access to operations that may affect the underlying system. Such operations are invoked by the Ambari Agent process on Ambari Agent hosts, as the user executing the Ambari Agent process.

Mitigation: Ambari users should upgrade to version 2.4.2 or above.
Version 2.4.2 onwards properly enforces access based on required roles needed to execute custom commands.

Credit: Nitya Kumar Sharma from Microsoft

Fixed in Ambari 2.4.0

CVE-2014-3582: OpenSSL parameter injection vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.2.0 to 2.2.0

Versions Fixed: 2.4.0

Description: It may be possible to execute arbitrary system commands on the Ambari Sever host while generating SSL certificates for hosts in an Ambari cluster.

Mitigation: Ambari users should upgrade to version 2.4.0 or above.
Version 2.4.0 onwards properly enforces that agent-supplied host names are valid hostnames before attempting to execute OpenSSL commands to create SSL certificates. However, this feature may be disabled by setting security.agent.hostname.validate to "false" in the ambari.properties file. It is strongly recommended that the default value of security.agent.hostname.validate is not changed since it may enable this vulnerability.

Credit: David Jorm

CVE-2016-4976: Apache Ambari kadmin password visibility vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 2.0.0 to 2.2.2

Versions Fixed: 2.4.0

Description: Due to the way Ambari executes the kadmin command to manage principals in an MIT KDC, a user with access to the Ambari server host may be able to capture the KDC administrator credentials.

Mitigation: Ambari users should upgrade to version 2.4.0 or above.
Version 2.4.0 onwards sends passwords to the kadmin command via the command's STDIN channel rather then embed it as arguments in the executed command line.

Credit: Greg S. Senia from New York Life Insurance Company.

Fixed in Ambari 2.2.1

CVE-2016-0731: Ambari File Browser View security vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.7.0 to 2.2.0

Versions Fixed: 2.2.1

Description: Ambari File Browser View, depending on how it is configured, allows an Ambari admin user to gain access to Ambari Server's local file system.

Mitigation: Ambari users should upgrade to versions 2.2.1 or above.

Fixed in Ambari 2.1.2

CVE-2016-0707: File System Permissions aren't restrictive enough for the Agent/Command logs

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.7.0 to 2.1.1

Versions Fixed: 2.1.2

Description: Ambari agent's working folders (e.g. /var/lib/ambari-agent/data, /var/lib/ambari-agent/keys) do not have a restricted ACL. As the command log files may contain sensitive information, it will potentially allow access to un-authorized users.

Mitigation: Ambari users should use versions 2.1.2 or above to install new clusters. Version 2.1.2 onwards, ambari-agent work folders are associated with a restricted ACL. In addition, after upgrade to 2.1.2 or above, users should check and modify the ACLs of the existing folders as suggested.

- chmod -R 0600 /var/lib/ambari-agent/data
- chmod -R a+X /var/lib/ambari-agent/data
- chmod -R a+rx /var/lib/ambari-agent/data/tmp
- chmod 0600 /var/lib/ambari-agent/keys/*.key

CVE-2015-5210: Unvalidated Redirects and Forwards using targetURI parameter can enable phishing exploits

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.7.0 to 2.1.1

Versions Fixed: 2.1.2

Description: A redirect to an untrusted server is possible via unvalidated input that specifies a redirect URL upon successful login.

Mitigation: Ambari users should upgrade to version 2.1.2 or above. Version 2.1.2 onwards redirect locations must be relative URLs.

Fixed in Ambari 2.1.1

CVE-2015-3270: A non-administrative user can escalate themselves to have administrative privileges remotely

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.7.0, 2.0.0, 2.0.1, 2.1.0

Versions Fixed: 2.0.2, 2.1.1

Description: An authenticated user can remotely escalate his/her permissions to administrative level. This can escalate their privileges for access through the API as well from the UI.

Mitigation: Ambari users should upgrade to version 2.1.1 or above (2.0.0 and 2.0.1 can be upgraded to 2.0.2).

In fixed versions of Ambari (2.0.2; 2.1.1 and onward), access to the user resource endpoint is protected such that only a user with administrator privileges can esculate a user's privileges. A user, however, may still access the endpoint but may only change their own password.

Fixed in Ambari 2.1.0

CVE-2015-1775: Apache Ambari Server Side Request Forgery vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.5.0 to 2.0.2

Versions Fixed: 2.1.0

Description: Ambari exposes a proxy endpoint through “api/v1/proxy” that can be used make REST calls to arbitrary host:
port that are accessible from the Ambari server host. Ability to make these calls is limited to Ambari authenticated users only. In addition, an user need to b e Ambari admin user to make the REST calls using METHODs other than GET (non-
admin users can only call GET). This ability to call allows malicious users to perform port scans and/or access unsecured services visible to the Ambari Ser ver host through the proxy endpoint. In addition Ambari provides an utility to handle such proxy calls that are used by View instances hosted by Ambari

Mitigation: Ambari users should upgrade to version 2.1.0 or above. Version 2.1.0 onwards the proxy end point (api/v1
/proxy) has been disabled. In addition a configurable parameter (proxy.allowed.hostports) is introduced, in config file ambari.
properties, to explicitly specify a list of host/port that can be proxied to when using the utility.

Credit: This issue was discovered by Mateusz Olejarka (SecuRing).

CVE-2015-3186: Apache Ambari XSS vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: 1.7.0 to 2.0.2

Versions Fixed: 2.1.0

Description: Ambari allows authenticated cluster operator users to specify arbitrary text as a note when saving configuration changes. This note field is rendered as is (unescaped HTML). This exposes opportunities for XSS.

Mitigation: Ambari users should upgrade to version 2.1.0 or above.

Version 2.1.0 onwards properly HTML-escapes the note field associated with configuration changes.

Credit: Hacker Y on the Elephant Scale team.