Micro Focus Service Desk 7.2

March 2016

Novell

The information in this Readme pertains to the Micro Focus Service Desk 7.2.

1 What’s New

Micro Focus Service Desk 7.2 release comes with a new and improved portal including features such as KeyShield SSO integration, Item Reconciliation, and Telemetry.

For more information, see *What’s New in 7.2*.

2 Known Issues

2.1 When Strong Authentication is enabled the `application exception` error is displayed

When you enable the **Strong Authentication** option (**User** > **Teams** > **Team Name** > **Information** > **Details** > **Strong Authentication** and select **On**), the `application exception` error is displayed.

Workaround: None.

2.2 Service Desk does not support attachments that are more than 100 MB in size

When you try to download an attachment of more than 100 MB in size, then an `out of memory` error might be displayed.

Workaround: None

3 Security Fixes

Thanks to Pedro Ribeiro from Agile Information Security for discovering and reporting the following vulnerabilities:

- **CVE-2016-1593:** Fixed a path traversal vulnerability in the import users functionality that may have allowed a remote attacker authenticated as an administrative user to upload arbitrary files to the server. Depending on the payload and placement of the uploaded file, this could lead to remote code execution. For more information, see TID7017428.
- **CVE-2016-1594:** Fixed a vulnerability in the access control enforcement of the file download functionality that may have allowed a remote attacker authenticated as a non-privileged user to read arbitrary file attachments from other users in the system. For more information, see TID7017429.
- **CVE-2016-1595:** Fixed an HQL (Hibernate Query Language) injection vulnerability in the file download functionality that may have allowed a remote attacker authenticated as a non-privileged user to alter the HQL query being run against the database. This could lead to database information disclosure or download of arbitrary files from the server. For more information, see TID7017430.
- **CVE-2016-1596:** Fixed multiple stored cross site scripting vulnerabilities that may have allowed an attacker authenticated as a non-privileged user to inject arbitrary javascript into the context of other users' browser sessions (including administrative users). For more information, see TID7017431.

4 Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/. (https://www.novell.com/company/legal/).