Release Notes for Patch Release #4048

April 4, 2017

Security Patch Release

This Patch Release addresses critical vulnerabilities; please consider deploying it as soon as possible. Not deploying this Patch Release may result in remote service exploitation, security threats to users and exposure of sensitive data.

Detailed vulnerability descriptions will be publicly disclosed no earlier than five (5) working days after public availability of this Patch Release. There is no indication that one or more of these vulnerabilities are already getting exploited or that information about them is publicly circulating.

Copyright notice

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.8.1-rev34
Open-Xchange Office 7.8.1-rev11

Find more information about product versions and releases at `http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering`

2 Vulnerabilities fixed since previous Public Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Patch Release #3992. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

52255 CVE-2017-6912
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

51863 CVE-2017-6913
CVSS: 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

51667 CVE-2016-10078
CVSS: 3.6 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:L)

51622 CVE-2017-6912
CVSS: 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

3 Bugs fixed since previous Public Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Patch Release #3992.

51839 Certain serious (non UCE/UBE) HTML mail is not displayed
Too greedy check for possibly malicious content led to this issue.
This has been solved by allowing properly parsed start tag.

52518 Compatibility fix for Debian and systemd
The Debian project did rename the initial process from `systemd` to `init` when moving to Debian 8.7. Some areas of our startup scripts depend on this name to determine whether systemd is used or not. We're now querying `/proc/1/comm` to figure out the kind and name of process that takes care about inits.

4 Tests

Open-Xchange has successfully verified all bug fixes that could be reproduced within a lab environment.
To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server set-up for system and integration testing. All changes have been checked for potential side-effects and effect on behaviour. Unless explicitly stated within this document, we do not expect any side-effects.

5 Fixed Bugs

51839, 52518, 52255, 51863, 51667, 51622,