

Deskpro Security Incident

Christopher Nadeau - Comment (1) - Release Announcements - 2015-11-17

A couple of weeks ago, a file leakage vulnerability was discovered by a third-party security researcher doing an internal audit

This issue was reported privately by a responsible professional and we are confident that it was never "in the wild". We have no evidence that this bug was ever applied by a malicious user on any helpdesk

Affected Script

The vulnerability was found in a helper script (app/sys/scripts/testfile.php) used by our automated testing framework. It was meant for use by our QA tools and served no purpose in production. This affected DeskPRO On-Premise helpdesks (*not* Cloud) using builds between 323 and 425

This file and other types of internal system tools (such as diagnostic tools) are not accessible directly. They are only accessible through a specific "loader" URL. The "loader" was patched to disable access to the testfile.php script thereby fixing the vulnerability

Timeline

- 28th Oct 2015 10:46 GMT: Issue was reported •
- 28th Oct 2015 11:15 GMT: An updated distribution was released •
- 28th Oct 2015 12:08 GMT: We began to send emails to on-site customers •
- 30th Oct 2015 16:54 GMT: A follow-up email was sent to customers who had not upgraded yet •
- 17th Nov 2015 15:00 GMT: This posting was made public •

Securing your helpdesk

If you have not already, you *must* upgrade your DeskPRO helpdesk to the latest version. If you are using a version older than 426, then you are affected and must upgrade to remain safe

Now is also a good time to read our security guide in our sysadmin manual:

<https://manuals.deskpro.com/html/sysadmin/securing/securing.html>

.This guide goes over a few methods to add extra security to your On-Premise installation