# Deskpro Security Update (2019-09)

2019-10-01 - Christopher Nadeau - Comentário (1) - News

We released Deskpro v2019.8.0 today to on-premise customers to fix a critical security vulnerability. In this post, we will give you some background about the vulnerability and what we did to fix it, and what we're doing going forward.

## Timeline & How we learned of the vulnerability

We received a security advisory compiled by a professional security research firm. The report outlined how two separate bugs could be exploited together to achieve privilege escalation. Here's the timeline of events:

- Sunday, 22 September 2019 17:00: We were given a preliminary report from the researchers. The details were sparse, but we began investigating immediately while we waited for the full report to be compiled.
- Sunday, 22 September 2019 18:30: Our engineers figured out the root causes based on the preliminary report and had devised a fix.
- Sunday, 22 September 2019 18:40: The fix was deployed to our Cloud platform.
- Sunday, 22 September 2019 21:20: The full report was submitted to us. Our engineers were able to quickly confirm that the issues found by the researchers were resolved by our fix.
- Sunday, 22 September 2019 21:30: Our engineers were able to confirm that the vulnerability had never been exploited on our platform.
- The following week: Our engineers delved deep into the vulnerability to make 100% certain our fix was accurate. During this time we also spent time tightening permission checks in the code and adding extra assertions and tests to limit the impact should something like this ever happen again in the future.
- Tuesday, 1 October 2019 09:00: We rolled out v2019.8.0 to customers and sent out a general announcement email.

## About the vulnerability

We're classifying this as a *privilege escalation* vulnerability.

A privilege escalation vulnerability is a type of software fault which enables a user to exploit the system to obtain access that they normally wouldn't have. These kinds of vulnerabilities

can be caused by a number of different things: software bugs, configuration errors, even a simple oversight.

The vulnerability we discovered in Deskpro is based on a couple bugs that, if exploited in tandem in a certain way, could allow a user to impersonate an administrator.

#### How the exploit works

We're not going to detail how the vulnerability works just yet. We need to give customers a chance to upgrade and secure themselves before we share an example exploit.

## How Deskpro handles security issues

All software has bugs and unfortunately some of those bugs can sometimes manifest as security issues. Deskpro takes bug reports, especially those that touch on security, extremely seriously. We were able to identify, fix, and deploy the fix to our cloud platform within 90 minutes of the report being sent to us. We think that quick response time is key to keeping our customers safe.

Deskpro has operated a responsible disclosure program for years. In light of this incident, we're going a step further and will soon open a bug bounty program on HackerOne as well. These programs give security researchers a safe and secure method to submit sensitive bug reports to us in a way that benefits everyone.

But security starts with developers. Deskpro is built on frameworks and technologies that encourage safe practices, such as input sanitising and proven authentication/authorisation handling. There's always room for improvement though and we're reviewing our internal development procedures to see where we can improve. Things like more specific code review checklists or more automated fuzz testing -- extra checks like these can help prevent bugs from making it into production.

Comentário (1)

Comentário (1)

**Steve, Lam Hang**

há 4 anos

Excellent work staying on top of security.