CVE-2019-15006

Referaat

Autor: Andreas Vija

Tartu 2020
Käesolevaga luban Tartu Ülikoolil seda referaati avalikult eksponeerida kuni aastani 2023.

Andreas Vija

# Table of contents

Introduction .......................................................................................................................... 4
The vulnerability .................................................................................................................. 4
The threat ............................................................................................................................ 4
The fix................................................................................................................................. 5
Used sources....................................................................................................................... 6
Introduction

Confluence is a commercial work collaboration and document management system developed by the company Atlassian. On 4/12/2019 Twitter user SwiftOnSecurity noticed a behavior in Confluence that turned out to be a vulnerability potentially allowing a man-in-the-middle attack and was given the CVE ID CVE-2019-15006. By 12/12/2019 Atlassian had (mostly) fixed the issue.

The vulnerability

The vulnerability in question resided in the plugin Confluence Previews, which is used to communicate between the web applications Confluence Server and Confluence Data Center, and the client-side software Atlassian Companion.

The Confluence Previews plugin communicated with Atlassian Companion using a peculiar domain name atlassian-domain-for-localhost-connections-only.com. The DNS A record of this domain pointed to 127.0.0.1, meaning the current computer, where an Atlassian Companion local server was running.

The Atlassian Companion server contained an SSL certificate and the corresponding private key, used to enable Atlassian Companion to edit files using some local application and send the files back to Confluence.

The peculiar domain was a trick to allow using a certificate signed by a certificate authority for a local server. This is not an uncommon trick, but it is also not safe as it means that a certificate and its private key are publically distributed with the application’s source code.

The threat

Anyone using the application was potentially vulnerable to an attack, as a malicious party could extract the SSL certificate’s private key from the software’s source code without much effort. If an attacker was in the position to control their victim’s DNS resolution, they could carry out a
man-in-the-middle attack between Confluence Server or Confluence Data Center and Atlassian Companion.

This means that the attacker could redirect traffic, observing and modifying the communication as they wish. Therefore, not only could the user’s personal information and the content of private documents leak in this way, an attacker could potentially also change the documents.

Not only can this attack target single users, but carrying out this attack in a large network with many users is also entirely possible.

The fix

Atlassian has fixed the vulnerability by revoking the SSL certificate distributed with the Atlassian Companion application. This means that having maliciously extracted the certificate is no longer proof enough that the party presenting the certificate is who they claim to be.

Atlassian has also released updates for Confluence Server and Confluence Data Center, where the domain atlassian-domain-for-localhost-connections-only.com is no longer used.

This attack might still be possible for older versions of affected software however, if the attacker denied the victim access to certificate revocation information. As such updating software is still important.
Used sources


https://jira.atlassian.com/browse/CONFSERVER-59244

https://twitter.com/SwiftOnSecurity/status/1202034106495832067

https://www.theregister.co.uk/2019/12/05/atlassian_zero_day_bug/