External URLs [Update]

Fefe schreibt etwas über BigBlueButton, mit dem ich auch arbeite. „Wer da Präsentationen hochladen darf, hat Admin-Zugriff.“

Hanno Böck erklärt das näher: „BigBlueButton has a feature that lets a presenter upload a presentation in a wide variety of file formats that gets then displayed in the web application. This looked like a huge attack surface. The conversion for many file formats is done with Libreoffice on the server. Looking for ways to exploit server-side Libreoffice rendering I found a blog post by Bret Buerhaus that discussed a number of ways of exploiting such setups. One of the methods described there is a feature in Opendocument Text (ODT) files that allows embedding a file from an external URL in a text section. This can be a web URL like https or a file url and include a local file.“

Ich halte das in der Praxis nicht für dramatisch. Das schreibt Fefe auch: „Aber in diesem Fall musste gar kein Exploit her, denn die Dateiformate haben (völlig ohne Not, möchte ich

anmerken!) ein Feature, über das man externe Ressourcen über eine URL einbinden kann“. Ein Dozent, der anderen erlaubt, Dateien zu nutzen und hochzuladen, die bekannte Risiken haben, ist selbst schuld, wenn ihm die Sache um die Ohren fliegt.

[Update] Der beste aller Provider teilte mir mit, dass das Leck inzwischen abgedichtet sei.