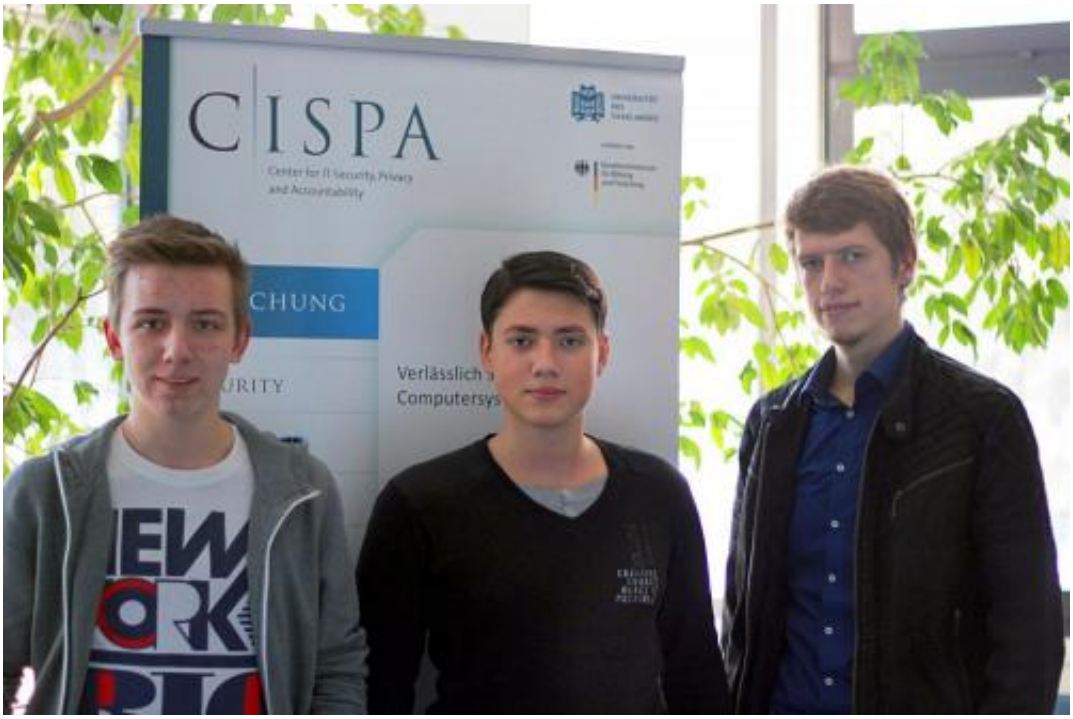
Cybersecurity students discover security gaps in 39,890 online databases

February 10 2015



Kai Greshake, Eric Petryka and Jens Heyens discovered 39,890 unprotected Internet databases. Credit: Saarland University

Anyone could call up or modify several million pieces of customer data online including names, addresses and e-mails. According to the Center for IT-Security, Privacy and Accountability (CISPA) in Saarbrücken, Germany, three of its students were able to show this for 40,000 online databases in both Germany and France. The cause is a misconfigured

open source database upon which millions of online stores and platforms from all over the world base their services.

If the operators blindly stick to the defaults in the installation process and do not consider crucial details, the data is available online, completely unprotected. CISPA has already contacted the vendor and data protection authorities.

"It is not a complex bug, but its effect is disastrous", explains Michael Backes, professor of information security and cryptography at Saarland University and director of CISPA. He was contacted by the students and CISPA employees Kai Greshake, Eric Petryka and Jens Heyens at the end of January. Heyens is a cybersecurity student at Saarland University, and his two fellow students plan to concentrate on this subject in the upcoming semester. The flaw which the three CISPA students detected affects 39,890 databases. "The databases are accessible online without being protected by any defensive mechanism. You even have the permissions to update and change data. Hence we assume that the databases were not left open on purpose", Backes explains. The vendor of the database is MongoDB Inc. Its database MongoDB is one of the most widely used open source databases worldwide. Out of curiosity, the students queried a publicly accessible search engine for servers and services connected to the Internet. In this manner, they discovered IP addresses companies use to run unprotected MongoDB databases.

When the students called up the detected MongoDB databases with the respective IP addresses, they were surprised: Access was neither locked, nor protected in any other way. "A database unprotected like this is similar to a public library with a wide open entrance door and without any librarian. Everybody can enter", explains Backes. Within a few minutes, the students detected this critical condition within numerous other databases as well. They even found a customer database which might belong to a French Internet service provider and mobile phone

carrier. It contained the addresses and telephone numbers of roughly eight million French customers. According to the students, among those addresses they also found the data of half a million German clients. They also detected the unprotected database of a German online retailer, including payment information. "The saved data can be used later to steal identities. Even if the identity theft is known, even years later the affected people have to deal with contracts signed under their own names by the identity thieves", says Backes. The CISPA researchers began contacting MongoDB Inc. immediately, as well as the international computer emergency response teams (CERTs). They informed the French data protection service Commission nationale de l'informatique et des libertés and the German Office for Information Security. "We do also hope that the developer of MongoDB will quickly include our results, incorporate them into its guidelines and forward them to the companies using the database", says Backes.

More information: cispa.saarland/wp-content/uplo … DB_documentation.pdf

Provided by Saarland University