Hacker Points to Weakness in LexisNexis Concordance

Other legal technology software vendors could face similar issues

By **Evan Koblentz** **Contact** **All Articles**

Law Technology News March 7, 2012

Image: clipart.com

A security weakness in the LexisNexis Concordance litigation support system could allow people to hijack database passwords, putting attorneys' client data at risk of theft, according to the hacker who discovered it. Concordance helps legal professionals import and manage trial documents, search and annotate data, and create custom case reports.

There have not been documented attacks based on the weakness, which is easily prevented **if customers follow Lexis' advice** to lock their databases. But many customers do not, and are left with Concordance running in its default, unlocked configuration.

Part of the reason this type of weakness exists is related to user behavior. Just as users of Facebook may wrongly assume their data is private, system administrators sometimes assume that security mechanisms are in place, or underestimate the ease with which unlocked databases can have their passwords defeated.

A white-hat hacker -- one who explores technology systems for research or curiosity, but not crime -- showed *Law Technology News* how Lexis' procedure for recovering lost Concordance database passwords is easily duplicated. The procedure works on all current versions of Concordance, including 8, 9, and 10. The hacker said he informed a Lexis-employed software trainer three years ago. The hacker declined to be identified.

Lexis officials confirmed the person's assertions of the method and timing. However, "We never, before or since, had any [other] feedback like this at all," said Matthew Gillis, Lexis' vice president and managing director, who leads the company's litigation and professional services division. "This is something that required [an administrator] level of access to do to begin with," he noted, referring to Concordance servers always residing behind network firewalls.

About 96 percent of Concordance customers use versions 8, 9, and 10, said Lexis officials, who declined to share the total number of customers, citing competitive reasons. However, the issue was not deemed serious enough to alert customers or to patch the software, they said.

The hacker disagrees with Lexis' assessment of the risk. Concordance has an emergency access method known as a back door -- program code intended to be very difficult for anyone except the software vendor to open, as a last resort to accessing data when passwords are lost. Back doors are common in enterprise software. But in Concordance, there are serious concerns about the ease with which that door can be opened and Lexis' reluctance to tighten it, the hacker explained.

"It was just based off of a theory that I had and some tools that I had on hand," the hacker said. "You don't

Find similar content

Firms mentioned

Companies, agencies mentioned

Key categories

Most viewed stories

Law Technology News Goin' Mobile With ALM

Lexis for Microsoft Office Now Works With Lexis Advance

EDRM Remains Vital to E-Discovery

Kirkland, Wachtell Lead on $6.9 Billion BMC Software Sale

Tech Circuit: Bay Bridge Edition

12 on 12: Tech Gifts for Mom

Interop Holds Court in Vegas, With Much to Offer Legal.

ALM Legal Intelligence Tracks Alternative Fee Arrangements, More News May 1 to 10

Bloomberg Names Compliance Chief After Client Data Breach

Redacted Emails Ordered Released in Aaron Swartz Case

have to be Mitnick," he joked, referring to infamous hacker **Kevin Mitnick**, who broke into several corporate networks, including IBM, Motorola, and Nokia. He served time in federal prison and was the subject of several books and movies.

If access to a Concordance **customer's network** is obtained, such as through remote infiltration using a computer virus, or through more direct means, like a lost laptop, then a hacker must then locate the correct database -- the organized collection of raw information that underpins all forms of e-discovery software. Doing so can be as simple as taking a process-of-elimination look at network servers and file directory names.

"I was trying to circumvent the security. Essentially when you set up the database, the password is stored internally on the database itself. I hacked it so I removed the password from the database. I wrote an executable file that tricked the database into thinking the password hadn't ever been set, so then you could go in and set the password yourself," the person explained.

The hacker described how the method works on any modern Concordance database, requiring no special programming. *Law Technology News* is withholding technical details of the software trick to avoid potentially endangering Concordance customer data.

CUSTOMERS REACT

One of Lexis' customers -- a litigation support manager at a large southern California firm, who asked not to be identified -- said the firm has used Concordance with approximately 300 databases for more than six years.

"I'm not totally shocked by that," the manager said, reacting to the password issue. "I don't think it was well thought-out on how [Lexis] set up the security section of it. I definitely would have, as a customer, wanted to know that, and would have wanted that fixed."

The law firm was confident in its network security, but there were other issues, such as users who could access the database by entering a user name without a password, the manager said. That's a problem because anyone who discovers or guesses someone's user name could then enter the Concordance system without authorization.

The firm stopped using Concordance two years ago because of such glitches, and now uses a kCura Relativity, the manager said.

Another customer, Fenwick & West CIO Matt Kesner, in San Francisco, said he's not surprised to hear of the weakness in Corcordance. "I don't think that law firms and law firm-specific software vendors have felt they needed to be particularly concerned about security."

"I think that all law firm products are going to need to get better. I hope that Lexis makes Concordance better," Kesner continued. "I think we all need to do better at security. The internet and law firm IT have been based on assumptions of trust that aren't necessarily apt in today's world."

Fenwick is safe because it locks its Concordance databases. Also, "We use white-hat hackers to test our system every six months," Kesner said, referring to the 300-attorney firm's network and servers. "We tell them, 'Go do your worst.' We try most of the traditional hacking routes plus we use social engineering," the latter approach referring to computer infiltration based on tricking people to reveal sensitive information instead of relying on technology alone.

Such **auditing and testing** is considered a leading-edge perspective that other large firms and corporations can emulate. Many computer hackers are not as ethical about their exploits as the person who discovered the Concordance issue, and they're often a step ahead of security software and service vendors.

Concordance competes against Lindon, Utah-based AccessData's **Summation**. Officials from AccessData declined to comment for this story.

WHAT NEXT?

Lexis has improved Concordance security to an extent, officials said. Gillis observed that Concordance 10, which shipped in summer 2009, has a stronger level of optional data encryption, known as SHA-1, than previous versions. Version 10 also saw the removal of a menu item called "Zap," which erases databases with only a single layer of confirmation. System administrators were encouraged to block that menu item, but it was enabled in the default configuration, which many firms do not change. Also, some customers

choose to subscribe to Lexis' professional services, which offers configuration assistance, Gillis added -- "That business is growing tremendously on the basis of what you're talking about," he said.

But the hacker said Lexis' recent changes are not enough, because his method is unrelated to encryption. Lexis could fix the password situation by using proven methods, the hacker said. "I know there's a way to have different libraries that are scrambled and pointing to different files," which is a way video game companies prevent their customers from sharing purchases, he said. The method uses what's called a process monitor. "If they had something implemented that looked to see if they had any process monitoring active, then it would shut down," and the password trick would not work.

Lexis officials also said security improvements for the forthcoming Concordance 11 are still being determined and could not be shared at this time.

Meanwhile, whether **Concordance Evolution**, a Lexis product launched last July that helps users manage large scale electronic data discovery, is affected by the hacker's method, and whether products from other legal technology vendors have similar weaknesses, are questions without clear answers. "It is a possibility," the hacker said. "I haven't had a chance to get my hands on other things."

"It's incredibly easy to defeat password schemes on many common applications, either cracking the password or simply bypassing it by overwriting the key space," legal technology consultant and *Law Technology News* editorial board member Craig Ball said. Although the hacker focused on Concordance, "I don't know that it's any worse than much else of what we see in law offices," Ball observed.

If other software companies' products share similar issues, they would not be alone. Several years ago, Microsoft began its "Patch Tuesday," a monthly cycle of security fixes, often followed by "Exploit Wednesday," when hackers rush to take advantage of unpatched systems. Mandiant, an Alexandria, Va., security firm, said it has seen 80 large law firms hacked since 2009, although officials declined to elaborate. Many large firms were cautioned recently by the New York office of the Federal Bureau of Investigation to be more vigilant in their network security, and there are even threats from nation-states, **according to recent** *Bloomberg* and *Forbes* reports.

Weaknesses in Concordance, or in litigation support and e-discovery products overall, probably do not exist in greater or lesser proportions than in any other major category of business software, the hacker observed. But as the technology becomes more mainstream, he said -- and increasingly full of client data -- its customers need to stay abreast of risks.

Evan Koblentz is a reporter for Law Technology News. Send **e-mail**.

From the Law.com Network