Researchers crack W3C encryption standard for XML

By Sean Gallagher | Published 6 months ago

There's new reason to be leery about relying on Web-based services to handle sensitive data. A pair of German researchers revealed at the ACM Conference on Computer and Communications Security in Chicago this week that they have discovered a way to decrypt data within XML documents that have been encrypted using an implementation of the World Wide Web Consortium's XML Encryption standard.

XML Encryption is used widely as part of server-to-server Web services connections to transmit secure information mixed with non-sensitive data, based on cipher-block chaining. It can be used, for example, to encrypt credit card information for a payment within an XML-based purchase order, so that the general data can be accessed by everyone who needs to have access to it while access to the financial data is limited to the people or systems authorized to process it.

But that encryption is apparently very weak, as Juraj Somorovsky and Tibor Jager of Ruhr University Bochum demonstrated. "We were able to decrypt data by sending modified ciphertexts to the server, by gathering information from the received error messages," the pair wrote in their paper, presented at ACM. They were able to demonstrate that the exploit worked on both a popular open-source implementation of W3C XML Encryption and on the implementation of every company that responded to their disclosure.

Fixing the vulnerability will require a total rewrite of the W3C standard. "There is no simple patch for this problem,” Somorovsky said in a statement issued by Ruhr University Bochum. “We therefore propose to change the standard as soon as possible.”