Researchers issue warning over Chrome extensions that access private data

September 6 2023, by Peter Grad

Credit: Pixabay/CC0 Public Domain

Google Chrome browser extensions expose users to hackers who can easily tap into their private data, including social security numbers, passwords and banking information, according to researchers at the University of Wisconsin-Madison (UW-M).

The researchers further uncovered vulnerabilities involving passwords that are stored in plain text within HTML source code on web sites of some of the world's largest corporate giants, including Google, Amazon, Citibank, Capital One and the Internal Revenue Service.

The problem stems from the manner in which extensions access internal web page code.

Google offers thousands of extensions that users install to handle calendar events, password management, ad blocking, email access, bookmark storage, translation and search activities.

While such extensions help expand upon browser capabilities and make browsing easier, they also expose stored data to intruders, said Asmit Nayak, a computer science graduate student at UW-M.

"In the absence of any protective measures, as seen on websites like IRS.gov, Capital One, USENIX, Google, and Amazon, sensitive data such as SSNs and credit card information are immediately accessible to all extensions running on the page," Nayak said in a report published on the pre-print server *arXiv* on Aug. 30. "This presents a significant security risk, as private data is left vulnerable."

The threat remains despite protective measures introduced by Google

this year that have been embraced by most browsers. The protocol placed stricter limits on what kinds of information extensions can access.

But there remains no protective layer between web pages and browser extensions, so bad actors can still evade detection.

The researchers described "the alarming discovery" of passwords stored in plain text HTML web page source files.

"A significant percentage of extensions possess the necessary permissions to exploit these vulnerabilities," Nayak said, adding that he and his two colleagues identified 190 extensions "that directly access password fields."

To test their suspicions about vulnerabilities, the researchers uploaded an extension that could exploit extension weakness and steal plain-text passwords from HTML pages of web sites. It contained no malicious code, so it passed security screening at Google's Chrome Web Store.

The ease with which the researchers uploaded a potentially harmful extension "underscores the urgent need for more robust security measures," Nayak said.

The researchers disabled the extension after they established it could bypass security measures and read restricted data.

Nayak said the extension faults stemmed from two key procedural violations in coding: least privilege and complete mediation.

Least privilege refers to the principle that users and systems should be granted only the lowest level of access privilege required to complete tasks. Any unnecessary privilege should be barred. Default access states

should be on "deny" and not "allow."

Complete mediation refers to evaluation of each and every access request, with no deviations or exceptions.

The researchers proposed two means to address the problem. The first is a JavaScript add-on for all extensions that provide solid cover for sensitive input fields.

The second proposal is to add a browser feature that alerts users when an attempt is made to access sensitive data.

The report, "Exposing and Addressing Security Vulnerabilities in Browser Text Input Fields," raised particular alarm over vulnerabilities at two major web sites.

"Major online marketplaces such as Google and Amazon do not implement any protections for credit card input fields," the report stated. "In these cases, credit card details, including the Security Code and zip code, are visible in plain text on the webpage. This presents a significant security risk, as any malicious extension could potentially access and steal this sensitive information."

The report continued, "The lack of protection on these websites is particularly concerning, given their scale and the volume of transactions they handle daily."

In repose to the report, an Amazon spokesperson said, "We encourage browser and extension developers to use security best practices to further protect customers using their services."

A Google spokesperson said they are looking into the matter.

More information: Asmit Nayak et al, Exposing and Addressing Security Vulnerabilities in Browser Text Input Fields, *arXiv* (2023). DOI: 10.48550/arxiv.2308.16321