Researcher Finds PayPal Password Vulnerability

January 15, 2020 - A security researcher by the name of Alex Birsan discovered method to expose the email addresses and passwords for PayPal accounts. The vulnerability, which has since been patched, could have left users of the service open to fraudulent activities.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The vulnerability would have taken significant technical ability to exploit, and there is no evidence that it was ever used. It also would have required victims to first visit a fraudulent PayPal page; something which probably could have been accomplished by through a phishing attack. Once that was done, hackers would have been able to access the impacted account and either drain it of funds or make purchases.

With all of that said, it appears that the real problem was the fact that PayPal was storing passwords in plain text, without any encryption. Had the passwords been encrypted, even if someone was able to access them due to the above-mentioned vulnerability, the passwords would have been unreadable. The same is true for the email addresses.

According to an article in Security Week, Birsan said it quite well. "â€œWhile this properly fixes the vulnerability, I believe that the whole thing could have been prevented when designing the system by following one of the oldest and most important pieces of infosec advice: Never store passwords in plain text."

After Birsan reported the problem to PayPal, the company patched the problem and then awarded Birsan $15,000 for his findings.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS