When people ask for security holes as features: Non-administrators reading other users' stuff

devblogs.microsoft.com/oldnewthing/20100405-00

April 5, 2010

Raymond Chen

Via the suggestion box, Aaron Lerch asks whether a non-administrator can retrieve/evaluate environment variables as they would appear for another user. This falls into the category of asking for a security hole as a feature, specifically an *information disclosure* security hole, because you are extracting information from a user's private data which has security access controls that do not grant everybody access. Generally speaking, users have full access to their data, as does the operating system itself, but nobody else. Administrators can get access to the data by taking ownership and modifying the ACL or using security overrides like `SeDebugPrivilege`, but that's the general idea. And certainly, unprivileged users don't have access to the data from other unprivileged users.

The way to get a user's initial environment variables is to call the `CreateEnvironmentBlock` function, passing the token of the user you are interested in. Note that it's more than just scraping the registry, because you also have to take into account group policy objects and the possibility that the information in the registry is incorrect because it is a stale cached roaming profile.

Raymond Chen

Follow