Microsoft Security Advisory 2269637 Released

By MSRC

Published: 2010-08-21 · Archived: 2026-04-05 20:28:08 UTC

Today we released MicrosoftSecurity Advisory 2269637. This is different from other Microsoft Security Advisories because it's not talking about specific vulnerabilities in Microsoft products. Rather, this is our official guidance in response to security research that has outlined a new, remote vector for a well-known class of vulnerabilities, known as DLL preloading or "binary planting" attacks. We are currently conducting a thorough investigation into how this new vector may affect Microsoft products. As always, if we find this issue affects any of our products, we will address them appropriately.

Additionally, today we are providing a defense-in-depth update that customers can deploy that will help protect against attempts to exploit vulnerable applications through this newly identified vector. Finally, we are using our strong connections with researchers and partners in the industry to help address this new class of vulnerability. Our Microsoft Vulnerability Research program has been working to coordinate communication between the researcher who first brought this new vector to us and other application developers who are affected by this issue.

What this new research demonstrates is a new remote vector for DLL preloading attacks. These attacks are not new or unique to the Windows platform. For instance, PATH attacks that are similar to this issue constitute some of the earliest class of attacks against the UNIX operating system. The attack focuses on tricking an application into loading a malicious library when it thinks it's loading a trusted library. For this to succeed, the application has to call the trusted library by name instead of properly using its full path (for example, calling dllname.dll rather than C:\Program Files\Common Files\Contoso\dllname.dll). The attacker then has to place a malicious copy of the library in a directory that the system will search to locate the library and have that be a directory it will search before the directory where the trusted library actually is. For example, if an attacker knows that the application simply calls for dllname.dll (rather than using the full path) and it will look for dllname.dll in the current working directory before looking in C:\Program Files\Common Files\Contoso\. Then if the attacker can plant a malicious copy of dllname.dll in the current working directory, the application will load it first executing the attacker's code in the application's security context.

PATH or DLL preloading attacks have so far required the attacker to plant the malicious library on the local client system. This new research outlines a way an attacker could levy these attacks by planting the malicious library on a network share. In this scenario, the attacker would create a data file that the vulnerable application would open, create a malicious library that the vulnerable application would use, post both of them on a network share that the user could access, and convince the user to open the data file. At that point, the application would load the malicious library and the attacker's code would execute on the user's system.

Because this is a new vector, rather than a new class of vulnerability, the existing best practices that protect against this class of vulnerability, automatically protect against this new vector: ensuring that applications make calls to trusted libraries using full path names.

While the best protection is following best practices, we are able to provide an additional layer of defense by offering a tool that can be configured to disable the loading of libraries from network shares. In particular, because this is altering functionality, we encourage customers to evaluate this tool before deploying it. As part of your evaluation, we encourage you to review the information at the Security Research and Defense (SRD) blog.

We will continue our work with the researchers and the industry to identify and address vulnerable applications. And as always, we will update you with any new information we have through our security advisories, security bulletins and the MSRC weblog as appropriate.

- Advisory
- Security
- Vulnerability
