

# Micro Focus Fortify

## Software Security Content

### Critical Advisory Support

**August 16, 2019**

Fortify Software Security Research is pleased to announce the immediate availability of the following update to Fortify WebInspect SecureBase:

#### **SAML Dupekey Injection (CVE-2019-1006)**

This update includes a check to detect a critical authorization bypass vulnerability in Microsoft WCF, WIF 3.5 and later in .NET Framework, WIF 1.0 component in Windows, WIF Nuget package, and WIF implementation in SharePoint. The check is identified by ID 11612. In order to use this check create a custom policy to run just this check, or add check ID 11612 to an existing policy, to include it in a scan. This vulnerability is also known as Dupe Key Confusion and is a type of XML Signature Verification Bypass that allows an attacker to insert an arbitrary signature into SAML token to gain unauthorized access to application, for privilege escalation and user impersonation. The vulnerability is identified by MITRE advisory CVE-2019-1006. It is recommended to upgrade vulnerable components to vendor recommended fix versions. Additional details about the vulnerability can be found in [whitepaper](#) released by the Micro Focus Software Security Research team at Blackhat 2019.



**Contact Fortify Technical Support**  
Micro Focus Fortify  
<https://softwaresupport.softwaregrp.com/>  
+1 (844) 260-7219



**Contact SSR**  
Alexander M. Hoole  
Manager, Software Security Research  
Micro Focus Fortify  
[hoole@microfocus.com](mailto:hoole@microfocus.com)  
+1 (650) 258-5916