Micro Focus

de segurança de software do Micro Focus FortifyAtualização **1 de 2019**

29.03.19

Sobre o Micro Focus Fortify Software Security Research

A equipe do Fortify Software Security Research converte pesquisa de ponta em inteligência de segurança que fortalece o portfólio de produtos Fortify, incluindo o Fortify Static Code Analyzer (SCA), o Fortify WebInspect e o Fortify Application Defender. Atualmente, o Conteúdo de segurança de software do Micro Focus Fortify oferece suporte a 999 categorias de vulnerabilidade em 25 linguagens de programação e se estende por mais de um milhão de APIs individuais.

Saiba mais em

https://software.microfocus.com/en-us/software/security-research

O Fortify Software Security Research (SSR) tem a satisfação de anunciar a disponibilidade imediata de atualizações para o Fortify Secure Coding Rulepacks (versão em inglês 2019.1.0), Fortify WebInspect SecureBase (disponível via SmartUpdate), Fortify Application Defender e Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Pacotes de regras de codificação segura do Fortify detectam 796 categorias únicas de vulnerabilidades em 25 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, a versão inclui o seguinte:

Angular 7[1]

O suporte para o Angular, incluindo o suporte de versões até e inclusive a versão 7.0.0, identifica fontes de entrada de um navegador e modela a validação de segurança realizada pelo Angular por padrão. Os modelos do Angular são estruturados de forma que todos os coletores regulares de JavaScript sejam compatíveis com projetos do Angular, incluindo a capacidade de encontrar categorias como Cross-Site Scripting: DDOM, Privacy Violation, problemas de avaliação de código dinâmico e muito mais.

Suporte à função AWS Lambda

Suporte às novas funções Lambda da Amazon Web Services (AWS) para as linguagens Java e Python. A funcionalidade permite que o fluxo de dados dos eventos de acionamento do Lambda na lógica da função correspondente, incluindo a cobertura de possíveis problemas de XSS quando o Lambda está conectado a um gateway de API.

AWS Java SDK v2

Novo suporte para o AWS Java SDK v2 para serviços S3 e DynamoDB. Inclui novas categorias, como:

- Access Control:ACL Manipulation
- Insecure Storage: S3 Full Anonymous Access
- Insecure Storage: S3 Read ACP Anonymous Access
- Insecure Storage: S3 Read Anonymous Access
- Insecure Storage: S3 Write Anonymous Access
- Insecure Storage: S3 Write ACP Anonymous Access
- NoSQL Injection: DynamoDB

Python Django[1]

Suporte atualizado para a Python Django Web Framework, incluindo suporte até a versão 2.1.7. As mudanças incluem suporte aprimorado de visualizações baseadas em classes e fluxos de dados associados, bem como suporte para funções/métodos do Django lançados desde o Django 1.8.

[1] O suporte para o Angular 7, Django e Wicket requer o Fortify SCA versão 19.1.0 ou posterior para garantir melhores resultados.

Apache Wicket[1]

Suporte aprimorado para o Apache Wicket Web Framework, incluindo suporte às versões 6, 7 e 8 da estrutura.

DISA STIG 4.9

Para dar suporte aos nossos clientes federais na área de conformidade, foi adicionada uma correlação do Micro Focus Fortify Taxonomy ao Application Security e ao Development STIG, versão 4.9, da Defense Information Systems Agency (DISA).

Micro Focus Fortify SecureBase [Fortify WebInspect]

O Fortify SecureBase combina verificações de milhares de vulnerabilidades com políticas que orientam os usuários nas seguintes atualizações disponíveis imediatamente pelo SmartUpdate:

Suporte a vulnerabilidades

Often Misused: File Upload

O widget jQuery File Upload da Blueimp foi considerado vulnerável à execução remota de código, conforme identificado pelo CVE-2018-9206. A vulnerabilidade permite que um invasor carregue e execute arquivos PHP arbitrários. Essa versão inclui uma verificação para detectar esta vulnerabilidade.

SQL Injection

Esta versão inclui aprimoramentos na verificação SQL Injection para incluir suporte a aplicativos que usam o Banco de Dados SQL do Microsoft Azure.

Sensitive Information Leak: External

Essa versão inclui uma verificação para detectar se o Magento CMS está sendo executado no modo de desenvolvedor. O modo de desenvolvedor destina-se ao uso em um ambiente de desenvolvimento ou teste. Ativar o modo de desenvolvedor em um ambiente de produção pode revelar dados importantes do aplicativo e do sistema para invasores em potencial e representar um risco de segurança.

Cross-Frame Scripting

O cabeçalho da diretiva *frame-ancestors* da Política de Segurança de Conteúdo fornece proteção de diretivas contra vulnerabilidades de Cross-Frame Scripting. Ele torna obsoleto o cabeçalho de HTTP X-Frame-Options atualmente em uso. Esta versão inclui melhorias na atual verificação de Cross-Frame Scripting para incluir suporte à diretiva frame-ancestors da Política de Segurança de Conteúdo.

Content Management System (CMS) Fingerprinting

Essa versão inclui melhorias na identificação da presença de um dos seguintes CMSs no servidor de destino durante uma varredura do WebInspect: WordPress, Drupal, Django, Joomla, Liferay, Magento, Sitecore, Sitefinity[2] e Umbraco. Uma verificação de informações é acionada para informar a descoberta.

Relatório de conformidade

DISA STIG 4.9

Para dar suporte aos nossos clientes federais na área de conformidade, esta versão contém uma correlação das verificações do WebInspect com a versão mais recente do Application Security e do Development STIG, versão 4.9, da Defense Information Systems Agency.

Atualizações da política

DISA STIG 4.9

Uma política personalizada para incluir verificações relevantes ao DISA STIG 4.9 foi adicionada à lista existente de políticas com suporte no WebInspect SecureBase.

Micro Focus Fortify Application Defender

O Fortify Application Defender é uma solução de autoproteção de aplicativos em tempo de execução (RASP) que ajuda as organizações a gerenciar e atenuar riscos provenientes de aplicativos de desenvolvimento interno ou de terceiros. Ele proporciona uma visibilidade centralizada no uso e abuso dos aplicativos, protegendo ao mesmo tempo as vulnerabilidades de software e outras infrações em tempo real. Para esta versão, a equipe de pesquisa de segurança da Micro Focus Fortify Software fornece as seguintes melhorias de recursos:

Injeção de expressão OGNL: Struts 2

Suporte expandido para detecção de injeção de expressão OGNL no Apache Struts 2, que cobre a vulnerabilidade crítica do Struts identificada pelo CVE-2018-11776. Os aplicativos que usam Apache Struts2 das versões 2.3.x até 2.3.34, ou das versões 2.5.x até 2.5.16, permitem que os invasores executem expressões OGNL arbitrárias se contiverem resultados de ação configurados sem namespace ou espaço de nomes curinga, e também se tiverem uma propriedade struts.mapper.alwaysSelectFullNamespace definida como verdadeira na configuração do struts.

[2] A detecção do Sitefinity exige WebInspect 19.1.0 ou posterior.

Micro Focus Fortify Premium Content

A equipe de pesquisa cria, estende e mantém uma variedade de recursos fora dos nossos principais produtos de inteligência de segurança.

DISA STIG 4.9[3]

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify SSC com suporte para o STIG 4.9 da DISA, que está disponível para download no Portal de suporte ao cliente do Fortify, em Conteúdo premium.

Micro Focus Fortify Taxonomy: Software Security Errors

O site do Fortify Taxonomy, que contém descrições para suporte de categoria recém-adicionadas, está disponível em https://vulncat.fortify.com. Os clientes que procuram o site anterior com a última atualização compatível podem acessá-lo no Portal de suporte do Micro Focus Fortify.

[3] O suporte para o relatório DISA STIG 4.9 requer o Fortify SSC versão 18.20 ou posterior.

Entre em contato com o suporte técnico do Fortify
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR de Contato
Alexander M. Hoole
Gerente de Software Security Research
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

29 de março de 2019