Micro Focus

Fortify Software Security Content

Atualização 1 de 2020

27 de março de 2020

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 Micro Focus Fortify Software Security Content oferece suporte a 1.019 categorias de vulnerabilidade em 26 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 2020.1.0), o Fortify WebInspect SecureBase (disponível via SmartUpdate) e o Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Fortify Secure Coding Rulepacks detectam 810 categorias únicas de vulnerabilidades em 26 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, esta versão inclui o seguinte:

Biblioteca de suporte padrão GoLang[1]

Biblioteca de suporte expandido para Go. O Go é uma linguagem de software livre estaticamente tipada projetada pelo Google, que visa facilitar a criação de software simples, confiável e eficiente. O Go é sintaticamente semelhante ao C, mas com mecanismos de segurança de memória, coleta de lixo e tipagem estrutural. Esta atualização abrange namespaces da biblioteca padrão principal e suporte para 53 tipos de vulnerabilidade, incluindo 19 categorias adicionais:

- Negação de serviço: Expressão regular
- Injeção de fórmula
- Erros de aleatoriedade
- Injeção de JSON
- Gerenciamento de chaves: Chave HMAC vazia
- Gerenciamento de chaves: Chave HMAC inserida em código fixo
- Falsificação de log
- Falsificação de log (debug)
- Injeção de recurso
- Hash de criptografia fraca
- Hash de criptografia fraca: Sal inserido em código fixo
- Hash de criptografia fraca: Sal controlado pelo usuário
- Assinatura de criptografia fraca: Tamanho de chave insuficiente
- Assinatura de criptografia fraca: Tamanho de chave controlado pelo usuário
- Criptografia fraca: Preenchimento RSA inadequado
- Criptografia fraca: Vetor de inicialização inseguro
- Criptografia fraca: Fluxo de codificação
- Criptografia fraca: Tamanho de chave controlado pelo usuário
- Injeção de XML

Erratas diversas

Nesta versão, continuamos a investir recursos para que possamos reduzir o número de problemas de falsos positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionados ao seguinte:

- As instâncias de JavaScript do "Cross-Site Scripting: DOM" que foram identificadas com maior precisão como self-XSS foram alteradas para a nova subcategoria "Cross-Site Scripting: Self", e agora são sinalizadas com prioridade mais baixa.
- No Java, devido a melhorias no mecanismo de modelagem, houve um aumento acidental do número de falsos positivos em código morto, especialmente em condições "se". As regras foram melhoradas de modo que um número significativo de problemas inválidos foi removido.

[1] É recomendada a versão SCA v20.1.0 ou posterior para melhorar os resultados de busca.

- Os raros problemas de desempenho relacionados a aplicativos JSP e Spring MVC foram resolvidos.
- Atualizações nos metadados externos para melhorar a correlação do Common Weakness Enumeration (CWE™) com o Micro Focus Fortify: Taxonomia de erros de segurança de software (também conhecidos como os 7 Reinos Perniciosos). As melhorias incluem o alinhamento de 41 IDs de CWE adicionais em 935 categorias na taxonomia de erros de segurança de software resultando em atualizações nos mapeamentos tanto no CWE quanto no CWE Top 25 2019. Necessariamente, quaisquer recursos relativos a relatórios e a filtragem "Agrupar por" pelo CWE serão afetados. Os IDs de CWE adicionais são os seguintes:
  CWE-88, CWE-97, CWE-119, CWE-147, CWE-192, CWE-203, CWE-212, CWE-266, CWE-267, CWE-276, CWE-279, CWE-280, CWE-346, CWE-347, CWE-436, CWE-506, CWE-527, CWE-529, CWE-530, CWE-531, CWE-536, CWE-540, CWE-541, CWE-548, CWE-550, CWE-705, CWE-775, CWE-799, CWE-917, CWE-921, CWE-923, CWE-925, CWE-926, CWE-937, CWE-942, CWE-1004, CWE-1021, CWE-1069, CWE-1173, CWE-1188, CWE-1236,

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

Inclusão de arquivo perigoso: Local

Uma vulnerabilidade grave que afeta o Tomcat usa a funcionalidade do protocolo AJP para obter acesso aos arquivos do servidor e permitir que um invasor leia ou inclua qualquer arquivo nos diretórios de aplicativos da web Apache Tomcat. Essa vulnerabilidade é conhecida como GhostCat e é reconhecida pelo CVE-2020-1938. Além disso, um ataque de execução de código arbitrário também pode ser feito. Esse problema afeta o Apache Tomcat 9.x (anterior ao 9.0.31), 8.x (anterior ao 8.5.51), 7.x (anterior ao 7.0.100) e todas as versões anteriores. Esta atualização do SecureBase inclui uma verificação para detectar essa vulnerabilidade.

Mapeamentos do Common Weakness Enumeration (CWE™):

O Common Weakness Enumeration (CWE™) é uma taxonomia de erros de software que podem causar vulnerabilidades no software. A taxonomia fornece uma maneira de consolidar a saída de diversas metodologias na avaliação de riscos e vulnerabilidades de software durante vários estágios do SDLC. Nesta versão, o SecureBase inclui mapeamentos atualizados de verificações para atualizações recentes no CWE. O CWE é uma taxonomia hierárquica. As verificações são mapeadas para o nó de folha mais próximo que corresponda ao objetivo da verificação.

Relatório de conformidade

Common Weakness Enumeration (CWE™) Top 25:

The Common Weakness Enumeration (CWE™) Top 25 com os erros de software mais perigosos (CWE Top 25) é uma lista criada pela MITRE. A lista apresenta as 25 categorias de vulnerabilidade mais comuns que podem causar vulnerabilidades no software. Esta atualização do SecureBase inclui mapeamentos para as seguintes categorias de CWE. Incluímos verificações que mapeiam diretamente a categoria identificada na CWE Top 25 ou um ID de CWE relacionado a um ID de CWE na lista dos Top 25 por meio do relacionamento "ChildOf".

Atualizações da política

Common Weakness Enumeration (CWE™)

The Common Weakness Enumeration (CWE™) Top 25 com os erros de software mais perigosos (CWE Top 25) é uma lista criada pela MITRE. A lista apresenta as 25 categorias de vulnerabilidade mais comuns que podem causar vulnerabilidades no software. Esta versão inclui uma política com uma lista de verificações para avaliar vulnerabilidades mapeadas no na CWE Top 25.

Erratas diversas:

Nesta versão, continuamos a investir recursos para que possamos reduzir o número de problemas de falsos positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionados ao seguinte:

- A correção de bugs na verificação de contrabando de solicitações HTTP reduz os falsos positivos relacionados à localização com a ID 11621. A verificação não considera mais o HTTP 405 como uma verificação válida de vulnerabilidade.
- Transporte inseguro: O conteúdo do relatório de codificação de SSL fraca agora inclui um exemplo para excluir as codificações do modo CBC, incluindo !SHA246 e !SHA384 na cadeia de caracteres de configuração. No entanto, recomendamos consultar o administrador do servidor para criar uma configuração do conjunto de codificação da lista branca forte.
- Correções adicionais no Insecure Transport: A detecção de codificação de SSL fraca foi feita para melhorar a detecção de configuração nos casos em que a verificação não conseguiu detectar codificações corretas em servidor compatível apenas com TLS1.2 e codificações fortes.

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.

OWASP Application Security Verification Standard (ASVS):

O Application Security Verification Standard (ASVS) é uma lista de requisitos e testes de segurança de aplicativos a serem executados durante o ciclo de vida de desenvolvimento de software (SDLC) e configuração para criar softwares seguros. Criamos mapeamentos de verificações do SecureBase e regras de SCA para os requisitos aplicáveis do padrão. No entanto, durante o processo de criação de correlações com nossos produtos, descobrimos instâncias em que os mapeamentos de CWE fornecidos pelo padrão podem ser aprimorados para se alinharem com mais precisão às verificações do SecureBase e às regras SCA. À medida que trabalhamos nessas melhorias, podemos disponibilizar esses artigos a clientes interessados, para avaliação e colaboração. Entre em contato com o SSR abaixo para obter o modelo e a política de conformidade para o WebInspect, ou um pacote de sementes SSC, se estiver interessado.

Micro Focus Fortify Taxonomy: Software Security Errors

O site 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 com suporte, podem acessá-lo no Portal de suporte do Micro Focus Fortify.

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

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

27 de março de 2020