

Experiência 1.1 - Common Weakness Enumeration (CWE)

A Common Weakness Enumeration (CWE) classifica classes de vulnerabilidade, atribuindo a cada classe de vulnerabilidades um identificador.

As vulnerabilidades de projecto:

Natureza	Tipo	Identidade	Nome
HasMembro	V	6	<u>Configuração incorreta de J2EE: comprimento de ID de sessão insuficiente</u>
HasMembro	V	7	<u>Configuração incorreta do J2EE: página de erro personalizada ausente</u>
HasMembro	V	8	<u>Configuração incorreta de J2EE: Bean de entidade declarado remoto</u>
HasMembro	V	9	<u>Configuração incorreta do J2EE: Permissões de acesso fracas para métodos EJB</u>
HasMembro	V	13	<u>Configuração incorreta do ASP.NET: senha no arquivo de configuração</u>
HasMembro	C	20	<u>Validação de entrada incorreta</u>
HasMembro	C	22	<u>Limitação indevida de um nome de caminho para um diretório restrito ('Traversal de caminho')</u>
HasMembro	V	24	<u>Caminho Traversal: '../filedir'</u>
HasMembro	B	36	<u>Travessia de caminho absoluto</u>
HasMembro	B	66	<u>Manipulação imprópria de nomes de arquivos que identificam recursos virtuais</u>
HasMembro	V	67	<u>Manipulação imprópria de nomes de dispositivos do Windows</u>
HasMembro	V	69	<u>Manuseio inadequado do Windows :: DATA Alternate Data Stream</u>
HasMembro	V	72	<u>Manipulação imprópria do caminho de fluxo de dados alternativo Apple HFS +</u>
HasMembro	C	73	<u>Controle Externo do Nome ou Caminho do Arquivo</u>
HasMembro	C	74	<u>Neutralização inadequada de elementos especiais na saída usada</u>

			<u>por um componente de Downstream ('Injection')</u>
HasMembro	(C)	75	<u>Falha na limpeza de elementos especiais em um plano diferente (injeção de elemento especial)</u>
HasMembro	(B)	76	<u>Neutralização indevida de elementos especiais equivalentes</u>
HasMembro	(C)	77	<u>Neutralização inadequada de elementos especiais usados em um comando ('Command Injection')</u>
HasMembro	(B)	78	<u>Neutralização indevida de elementos especiais usados em um comando do sistema operacional ('injeção de comando do sistema operacional')</u>
HasMembro	(B)	79	<u>Neutralização incorreta de entrada durante a geração de páginas da Web ('Cross-site Scripting')</u>
HasMembro	(V)	84	<u>Neutralização inadequada de esquemas de URI codificados em uma página da Web</u>
HasMembro	(B)	88	<u>Injeção ou modificação de argumento</u>
HasMembro	(B)	89	<u>Neutralização indevida de elementos especiais usados em um comando SQL ('SQL Injection')</u>
HasMembro	(B)	90	<u>Neutralização indevida de elementos especiais usados em uma consulta LDAP ('LDAP Injection')</u>
HasMembro	(B)	91	<u>Injeção de XML (também conhecido como Injeção XPath Cega)</u>
HasMembro	(B)	93	<u>Neutralização Incorreta das Sequências CRLF ('CRLF Injection')</u>
HasMembro	(C)	94	<u>Controle indevido de geração de código ('Code Injection')</u>
HasMembro	(B)	95	<u>Neutralização Indevida de Diretivas em Código Avaliada Dinamicamente ('Injeção de Eval')</u>
HasMembro	(B)	96	<u>Neutralização indevida de diretivas em código salvo estaticamente ('Injeção de código estático')</u>
HasMembro	(V)	97	<u>Neutralização incorreta de inclusões</u>

			<u>do lado do servidor (SSI) em uma página da Web</u>
HasMembro	● B	98	<u>Controle inadequado de nome de arquivo para incluir / exigir declaração no programa PHP ('PHP Remote File Inclusion')</u>
HasMembro	● B	99	<u>Controle impróprio de identificadores de recursos ('Injeção de recursos')</u>
HasMembro	● B	115	<u>Interpretação errada da entrada</u>
HasMembro	● C	116	<u>Codificação imprópria ou escape de saída</u>
HasMembro	● C	118	<u>Acesso incorreto do recurso indexável ('Erro de intervalo')</u>
HasMembro	● C	119	<u>Restrição indevida de operações dentro dos limites de um buffer de memória</u>
HasMembro	● V	121	<u>Estouro de buffer com base em pilha</u>
HasMembro	● V	122	<u>Excesso de buffer com base em heap</u>
HasMembro	● B	124	<u>Underwrite de buffer ('Buffer Underflow')</u>
HasMembro	● B	130	<u>Manipulação imprópria da inconsistência de parâmetro de comprimento</u>
HasMembro	● B	184	<u>Lista negra incompleta</u>
HasMembro	● B	188	<u>Confiança no layout de dados / memória</u>
HasMembro	● B	198	<u>Uso de pedidos incorretos de bytes</u>
HasMembro	● C	200	<u>Exposição de informação</u>
HasMembro	● V	202	<u>Exposição de dados confidenciais por meio de consultas de dados</u>
HasMembro	● C	203	<u>Exposição da informação através da discrepância</u>
HasMembro	● B	204	<u>Exposição da informação da discrepancia da resposta</u>
HasMembro	● B	205	<u>Exposição da informação através da discrepancia comportamental</u>
HasMembro	● V	206	<u>Exposição da informação do estado interno através da inconsistência comportamental</u>
HasMembro	● V	207	<u>Exposição da informação através de</u>

			<u>uma inconsistência comportamental externa</u>
HasMembro	(B)	208	<u>Exposição da informação através da discrepância de tempo</u>
HasMembro	(B)	209	<u>Exposição da informação através de uma mensagem de erro</u>
HasMembro	(B)	210	<u>Exposição da informação através da mensagem de erro autogerada</u>
HasMembro	(B)	211	<u>Exposição da informação através da mensagem de erro gerada externamente</u>
HasMembro	(B)	212	<u>Remoção transfronteiriça imprópria de dados confidenciais</u>
HasMembro	(B)	213	<u>Exposição intencional de informações</u>
HasMembro	(V)	214	<u>Exposição da informação através do ambiente do processo</u>
HasMembro	(V)	215	<u>Exposição de informações através de informações de depuração</u>
HasMembro	(C)	216	<u>Erros de contenção (erros de contêiner)</u>
HasMembro	(V)	220	<u>Dados confidenciais sob a raiz do FTP</u>
HasMembro	(C)	221	<u>Perda de informação ou omissão</u>
HasMembro	(B)	222	<u>Truncamento de informações relevantes para segurança</u>
HasMembro	(B)	223	<u>Omissão de informações relevantes para a segurança</u>
HasMembro	(B)	224	<u>Informações relevantes sobre segurança obscuras por nome alternativo</u>
HasMembro	(B)	226	<u>Informações confidenciais não esclarecidas antes do lançamento</u>
HasMembro	(C)	228	<u>Manipulação imprópria da estrutura sintaticamente inválida</u>
HasMembro	(B)	229	<u>Manipulação imprópria de valores</u>
HasMembro	(V)	232	<u>Manipulação imprópria de valores indefinidos</u>
HasMembro	(B)	233	<u>Manipulação imprópria de parâmetros</u>
HasMembro	(V)	234	<u>Falha ao lidar com o parâmetro</u>

			<u>ausente</u>
HasMembro	● V	236	<u>Manipulação indevida de parâmetros indefinidos</u>
HasMembro	● V	238	<u>Manipulação imprópria de elementos estruturais incompletos</u>
HasMembro	● V	239	<u>Falha ao lidar com elemento incompleto</u>
HasMembro	● B	240	<u>Manipulação imprópria de elementos estruturais inconsistentes</u>
HasMembro	● B	241	<u>Manipulação imprópria do tipo de dados inesperados</u>
HasMembro	● V	245	<u>Boas Práticas do J2EE: Gerenciamento Direto de Conexões</u>
HasMembro	● V	246	<u>Boas Práticas do J2EE: Uso Direto dos Soquetes</u>
HasMembro	● C	250	<u>Execução com Privilégios Desnecessários</u>
HasMembro	● V	256	<u>Armazenamento Desprotegido de Credenciais</u>
HasMembro	● B	257	<u>Armazenando senhas em um formato recuperável</u>
HasMembro	● V	258	<u>Senha vazia no arquivo de configuração</u>
HasMembro	● B	259	<u>Uso de senha codificada</u>
HasMembro	● V	260	<u>Senha no arquivo de configuração</u>
HasMembro	● V	261	<u>Criptografia fraca para senhas</u>
HasMembro	● V	262	<u>Não usando o envelhecimento da senha</u>
HasMembro	● B	263	<u>Envelhecimento da Senha com Longa Expiração</u>
HasMembro	● B	266	<u>Atribuição de Privilégio Incorreta</u>
HasMembro	● B	267	<u>Privilégio Definido com Ações Não Seguras</u>
HasMembro	● B	268	<u>Encadeamento de Privilégios</u>
HasMembro	● C	269	<u>Gerenciamento impróprio de privilégios</u>
HasMembro	● B	270	<u>Erro de comutação de contexto de privilégio</u>
HasMembro	● C	271	<u>Erros de queda / redução de privilégios</u>

HasMembro		272	<u>Violação pelo Menor Privilégio</u>
HasMembro		273	<u>Verificação imprópria para privilégios descartados</u>
HasMembro		274	<u>Manipulação imprópria de privilégios insuficientes</u>
HasMembro		276	<u>Permissões padrão incorretas</u>
HasMembro		277	<u>Permissões herdadas inseguras</u>
HasMembro		278	<u>Permissões herdadas preservadas inseguras</u>
HasMembro		279	<u>Permissões atribuídas à execução incorreta</u>
HasMembro		280	<u>Manipulação indevida de permissões ou privilégios insuficientes</u>
HasMembro		281	<u>Preservação indevida de permissões</u>
HasMembro		282	<u>Gestão inadequada de propriedade</u>
HasMembro		283	<u>Propriedade não verificada</u>
HasMembro		284	<u>Controle de Acesso Impróprio</u>
HasMembro		285	<u>Autorização Indevida</u>
HasMembro		286	<u>Gerenciamento incorreto de usuários</u>
HasMembro		287	<u>Autenticação Inadequada</u>
HasMembro		288	<u>Desvio de autenticação usando um caminho ou canal alternativo</u>
HasMembro		289	<u>Bypass de Autenticação por Nome Alternativo</u>
HasMembro		290	<u>Bypass de Autenticação por Spoofing</u>
HasMembro		291	<u>Confiança no endereço IP para autenticação</u>
HasMembro		293	<u>Usando o campo de referência para autenticação</u>
HasMembro		294	<u>Bypass de Autenticação por Capture-replay</u>
HasMembro		295	<u>Validação incorreta de certificado</u>
HasMembro		296	<u>Seguimento impróprio da cadeia de confiança de um certificado</u>
HasMembro		297	<u>Validação imprópria de certificado com incompatibilidade de host</u>
HasMembro		298	<u>Validação imprópria da validade do certificado</u>
HasMembro		299	<u>Verificação indevida de revogação de certificado</u>

HasMembro		300	<u>Canal Acessível por Non-Endpoint ('Man-in-the-middle')</u>
HasMembro		301	<u>Ataque de Reflexão em um Protocolo de Autenticação</u>
HasMembro		302	<u>Bypass de Autenticação por Dados Assumidos-Imutáveis</u>
HasMembro		304	<u>Etapa crítica ausente na autenticação</u>
HasMembro		305	<u>Bypass de Autenticação por Fraqueza Primária</u>
HasMembro		306	<u>Autenticação ausente para função crítica</u>
HasMembro		307	<u>Restrição Indevida de Tentativas de Autenticação Excessiva</u>
HasMembro		308	<u>Uso de Autenticação de fator único</u>
HasMembro		309	<u>Uso do Sistema de Senha para Autenticação Primária</u>
HasMembro		311	<u>Ausência de criptografia de dados confidenciais</u>
HasMembro		312	<u>Armazenamento em texto não criptografado de informações confidenciais</u>
HasMembro		313	<u>Armazenamento de texto não criptografado em um arquivo ou no disco</u>
HasMembro		314	<u>Armazenamento de texto não criptografado no registro</u>
HasMembro		315	<u>Armazenamento em texto não criptografado de informações confidenciais em um cookie</u>
HasMembro		316	<u>Armazenamento de texto não criptografado de informações confidenciais na memória</u>
HasMembro		317	<u>Armazenamento em texto não criptografado de informações confidenciais na GUI</u>
HasMembro		318	<u>Armazenamento em texto não criptografado de informações confidenciais no executável</u>
HasMembro		319	<u>Transmissão por texto não criptografado de informações</u>

			<u>confidenciais</u>
HasMembro	(B)	321	<u>Uso de chave criptográfica embutida</u>
HasMembro	(B)	322	<u>Troca de Chaves sem Autenticação de Entidade</u>
HasMembro	(B)	323	<u>Reutilizando um Nonce, par de chaves na criptografia</u>
HasMembro	(B)	324	<u>Uso de uma chave após sua data de expiração</u>
HasMembro	(B)	325	<u>Etapa criptográfica necessária ausente</u>
HasMembro	(C)	326	<u>Força de criptografia inadequada</u>
HasMembro	(B)	327	<u>Uso de Algoritmo Criptográfico Quebrado ou Arriscado</u>
HasMembro	(B)	328	<u>Hash reversível de sentido único</u>
HasMembro	(V)	329	<u>Não usando um Random IV com o modo CBC</u>
HasMembro	(C)	330	<u>Uso de valores aleatórios insuficientes</u>
HasMembro	(B)	331	<u>Entropia insuficiente</u>
HasMembro	(V)	332	<u>Entropia insuficiente no PRNG</u>
HasMembro	(V)	333	<u>Manipulação indevida de entropia insuficiente no TRNG</u>
HasMembro	(B)	334	<u>Pequeno espaço de valores aleatórios</u>
HasMembro	(B)	335	<u>Uso Incorreto de Sementes no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro	(B)	336	<u>Mesma Semente no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro	(B)	337	<u>Semente Previsível no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro	(B)	338	<u>Uso do Gerador de Números Pseudo-Randomizados Criptograficamente Fracos (PRNG)</u>
HasMembro	(B)	339	<u>Espaço Pequeno de Semente no PRNG</u>
HasMembro	(C)	340	<u>Problemas de Previsibilidade</u>
HasMembro	(B)	341	<u>Previsível do estado observável</u>
HasMembro	(B)	342	<u>Valor Exato Previsível dos Valores Anteriores</u>

HasMembro		343	<u>Intervalo de valores previsíveis dos valores anteriores</u>
HasMembro		344	<u>Uso de valor invariante em contexto dinamicamente variável</u>
HasMembro		345	<u>Verificação insuficiente de autenticidade de dados</u>
HasMembro		346	<u>Erro de validação de origem</u>
HasMembro		347	<u>Verificação imprópria da assinatura criptográfica</u>
HasMembro		348	<u>Uso de menor fonte confiável</u>
HasMembro		349	<u>Aceitação de dados não confiáveis irrelevantes com dados confiáveis</u>
HasMembro		350	<u>Confiança na resolução reversa de DNS para uma ação crítica de segurança</u>
HasMembro		352	<u>Falsificação de Solicitação Entre Sites (CSRF)</u>
HasMembro		353	<u>Suporte ausente para verificação de integridade</u>
HasMembro		354	<u>Validação imprópria do valor de verificação de integridade</u>
HasMembro		356	<u>A interface do usuário do produto não avisa o usuário de ações não seguras</u>
HasMembro		357	<u>Aviso de IU insuficiente de operações perigosas</u>
HasMembro		358	<u>Verificação de segurança incorretamente implementada para padrão</u>
HasMembro		359	<u>Exposição de Informações Privadas ('Violação de Privacidade')</u>
HasMembro		360	<u>Confiança dos dados do evento do sistema</u>
HasMembro		362	<u>Execução Concorrente usando Recurso Compartilhado com Sincronização Indevida ('Condição de Corrida')</u>
HasMembro		363	<u>Condição de Corrida Habilitando Link Following</u>
HasMembro		364	<u>Condição de corrida de manipulador</u>

			<u>de sinal</u>
HasMembro	● B	366	<u>Condição de corrida dentro de um segmento</u>
HasMembro	● B	368	<u>Condição de Corrida de Comutação de Contexto</u>
HasMembro	● V	370	<u>Verificação ausente da revogação de certificado após a verificação inicial</u>
HasMembro	● B	372	<u>Distinção Incompleta do Estado Interno</u>
HasMembro	● B	377	<u>Arquivo temporário inseguro</u>
HasMembro	● B	378	<u>Criação de arquivo temporário com permissões inseguras</u>
HasMembro	● B	379	<u>Criação de arquivo temporário no diretório com permissões incorretas</u>
HasMembro	● V	383	<u>Boas práticas do J2EE: uso direto de threads</u>
HasMembro	● ● B	384	<u>Fixação de sessão</u>
HasMembro	● B	385	<u>Canal de temporização secreto</u>
HasMembro	● B	386	<u>Nome simbólico não mapeando para corrigir o objeto</u>
HasMembro	● C	390	<u>Detecção da condição de erro sem ação</u>
HasMembro	● B	391	<u>Condição de erro não verificado</u>
HasMembro	● B	392	<u>Relatório de falta de condição de erro</u>
HasMembro	● B	393	<u>Retorno do Código de Status Errado</u>
HasMembro	● B	394	<u>Código de status inesperado ou valor de retorno</u>
HasMembro	● B	396	<u>Declaração de captura para exceção genérica</u>
HasMembro	● B	397	<u>Declaração de lançamentos para exceção genérica</u>
HasMembro	● C	400	<u>Consumo Descontrolado de Recursos ('Exaustão de Recursos')</u>
HasMembro	● B	401	<u>Liberação incorreta de memória antes de remover a última referência ('Memory Leak')</u>
HasMembro	● C	402	<u>Transmissão de recursos privados em uma nova esfera ('vazamento de recursos')</u>

HasMembro	(B)	403	<u>Exposição do descritor de arquivo à esfera de controle não intencional ('vazamento de descritor de arquivo')</u>
HasMembro	(B)	404	<u>Encerramento ou Liberação Indevida de Recursos</u>
HasMembro	(C)	405	<u>Consumo de Recursos Assimétricos (Amplificação)</u>
HasMembro	(B)	406	<u>Controle insuficiente de volume de mensagens de rede (amplificação de rede)</u>
HasMembro	(B)	407	<u>Complexidade algorítmica</u>
HasMembro	(B)	408	<u>Ordem de Comportamento Incorreta: Amplificação Antecipada</u>
HasMembro	(B)	409	<u>Manipulação imprópria de dados altamente compactados (amplificação de dados)</u>
HasMembro	(B)	410	<u>Pool de recursos insuficiente</u>
HasMembro	(B)	412	<u>Bloqueio Acessível Externamente Irrestrito</u>
HasMembro	(B)	413	<u>Bloqueio impróprio de recursos</u>
HasMembro	(B)	414	<u>Verificação de bloqueio ausente</u>
HasMembro	(V)	415	<u>Double Free</u>
HasMembro	(B)	416	<u>Use After Free</u>
HasMembro	(B)	419	<u>Canal principal desprotegido</u>
HasMembro	(B)	420	<u>Canal alternativo desprotegido</u>
HasMembro	(B)	421	<u>Condição de corrida durante o acesso ao canal alternativo</u>
HasMembro	(V)	422	<u>Canal de Mensagens do Windows Desprotegido ('Shatter')</u>
HasMembro	(C)	424	<u>Proteção inadequada do caminho alternativo</u>
HasMembro	(B)	425	<u>Solicitação Direta ('Navegação Forçada')</u>
HasMembro	(B)	426	<u>Caminho de pesquisa não confiável</u>
HasMembro	(B)	432	<u>Manipulador de sinal perigoso não desativado durante operações confidenciais</u>
HasMembro	(B)	434	<u>Upload irrestrito de arquivo com tipo perigoso</u>

HasMembro		435	<u>Interação imprópria entre várias entidades que se comportam corretamente</u>
HasMembro		436	<u>Interpretação Conflito</u>
HasMembro		437	<u>Modelo Incompleto de Recursos de Ponto Final</u>
HasMembro		439	<u>Mudança Comportamental em Nova Versão ou Ambiente</u>
HasMembro		440	<u>Violação esperada de comportamento</u>
HasMembro		441	<u>Proxy ou intermediário involuntário ("adjunto confuso")</u>
HasMembro		444	<u>Interpretação Inconsistente de Pedidos HTTP ('HTTP Request Smuggling')</u>
HasMembro		446	<u>Discrepância da interface do usuário para o recurso de segurança</u>
HasMembro		447	<u>Recurso não implementado ou não suportado na interface do usuário</u>
HasMembro		450	<u>Múltiplas Interpretações da Entrada da Interface do Usuário</u>
HasMembro		451	<u>Interface do usuário (IU) Deturpação de informações críticas</u>
HasMembro		453	<u>Inicialização de Variável Padrão Insegura</u>
HasMembro		454	<u>Inicialização Externa de Variáveis Confiáveis ou Armazenamentos de Dados</u>
HasMembro		455	<u>Não-saída na inicialização com falha</u>
HasMembro		459	<u>Limpeza Incompleta</u>
HasMembro		462	<u>Chave Duplicada na Lista Associativa (Alist)</u>
HasMembro		463	<u>Exclusão da estrutura de dados Sentinel</u>
HasMembro		464	<u>Adição de estrutura de dados Sentinel</u>
HasMembro		466	<u>Retorno do valor do ponteiro fora do intervalo esperado</u>
HasMembro		470	<u>Uso de entrada controlada externamente para selecionar</u>

			<u>classes ou código ('Reflexão insegura')</u>
HasMembro	● B	471	<u>Modificação de Dados Assumidos-Imutáveis (MAID)</u>
HasMembro	● B	474	<u>Uso de função com implementações inconsistentes</u>
HasMembro	● B	475	<u>Comportamento indefinido para entrada na API</u>
HasMembro	● V	479	<u>Uso de manipulador de sinal de uma função não reentrante</u>
HasMembro	● B	494	<u>Download do código sem verificação de integridade</u>
HasMembro	● B	501	<u>Confiança de violação de limite</u>
HasMembro	● V	502	<u>Desserialização de dados não confiáveis</u>
HasMembro	● B	510	<u>Alçapão</u>
HasMembro	● B	511	<u>Lógica / Time Bomb</u>
HasMembro	● B	512	<u>Spyware</u>
HasMembro	● V	520	<u>Configuração incorreta do .NET: uso de falsificação de identidade</u>
HasMembro	● B	521	<u>Requisitos de senha fraca</u>
HasMembro	● B	522	<u>Credenciais insuficientemente protegidas</u>
HasMembro	● V	523	<u>Transporte Desprotegido de Credenciais</u>
HasMembro	● V	526	<u>Exposição da informação através de variáveis ambientais</u>
HasMembro	● V	532	<u>Exposição de informações através de arquivos de log</u>
HasMembro	● V	535	<u>Exposição da informação através da mensagem de erro do escudo</u>
HasMembro	● V	539	<u>Exposição da informação através de cookies persistentes</u>
HasMembro	● B	544	<u>Mecanismo de tratamento de erros padronizado ausente</u>
HasMembro	● V	554	<u>Configuração incorreta do ASP.NET: não usando o Input Validation Framework</u>
HasMembro	● V	555	<u>Configuração incorreta de J2EE: Senha de texto sem formatação no</u>

			<u>arquivo de configuração</u>
HasMembro	V	564	<u>Injeção de SQL: Hibernate</u>
HasMembro	B	565	<u>Confiança em Cookies sem Validação e Verificação de Integridade</u>
HasMembro	V	566	<u>Bypass de Autorização Através da Chave Primária SQL Controlada pelo Usuário</u>
HasMembro	B	567	<u>Acesso não sincronizado a dados compartilhados em um contexto multithread</u>
HasMembro	V	574	<u>Práticas ruins do EJB: uso de primitivas de sincronização</u>
HasMembro	V	575	<u>Boas Práticas do EJB: Uso do AWT Swing</u>
HasMembro	V	576	<u>Boas Práticas do EJB: Uso de Java I / O</u>
HasMembro	V	577	<u>Boas Práticas do EJB: Uso de Soquetes</u>
HasMembro	V	578	<u>Práticas incorretas do EJB: uso do carregador de classes</u>
HasMembro	V	579	<u>Práticas ruins do J2EE: objeto não serializável armazenado na sessão</u>
HasMembro	B	587	<u>Atribuição de um endereço fixo a um ponteiro</u>
HasMembro	V	588	<u>Tentativa de acessar filho de um ponteiro de estrutura não</u>
HasMembro	V	589	<u>Chamada para API não onipresente</u>
HasMembro	V	593	<u>Bypass de Autenticação: Objeto OpenSSL CTX Modificado Após a Criação dos Objetos SSL</u>
HasMembro	V	594	<u>J2EE Framework: Salvando Objetos Não Serializáveis no Disco</u>
HasMembro	V	598	<u>Exposição de informações através de seqüências de caracteres de consulta no pedido GET</u>
HasMembro	V	599	<u>Validação perdida do certificado OpenSSL</u>
HasMembro	V	601	<u>Redirecionamento de URL para site não confiável ('Redirecionamento aberto')</u>

HasMembro		602	<u>Imposição do lado do cliente da segurança do lado do servidor</u>
HasMembro		603	<u>Uso da Autenticação do Lado do Cliente</u>
HasMembro		605	<u>Múltiplas Vinculações à Mesma Porta</u>
HasMembro		610	<u>Referência externamente controlada a um recurso em outra esfera</u>
HasMembro		612	<u>Exposição de informação através da indexação de dados privados</u>
HasMembro		613	<u>Expiração de sessão insuficiente</u>
HasMembro		618	<u>Método ActiveX não seguro exposto</u>
HasMembro		620	<u>Alteração de senha não confirmada</u>
HasMembro		623	<u>Controle inseguro do ActiveX marcado como seguro para script</u>
HasMembro		636	<u>Não falhando com segurança ('Failing Open')</u>
HasMembro		637	<u>Complexidade Desnecessária no Mecanismo de Proteção (Não Usando a "Economia do Mecanismo")</u>
HasMembro		638	<u>Não usando mediação completa</u>
HasMembro		639	<u>Bypass de Autorização Através da Chave Controlada pelo Usuário</u>
HasMembro		640	<u>Mecanismo de recuperação de senha fraca para senha esquecida</u>
HasMembro		641	<u>Restrição Incorreta de Nomes para Arquivos e Outros Recursos</u>
HasMembro		642	<u>Controle Externo de Dados Críticos do Estado</u>
HasMembro		644	<u>Neutralização incorreta de cabeçalhos HTTP para sintaxe de script</u>
HasMembro		645	<u>Mecanismo de bloqueio de conta excessivamente restritivo</u>
HasMembro		646	<u>Confiança no nome do arquivo ou na extensão do arquivo fornecido externamente</u>
HasMembro		647	<u>Uso de Caminhos de URL Não-Canônicos para Decisões de Autorização</u>
HasMembro		648	<u>Uso incorreto de APIs privilegiadas</u>

HasMembro		649	<u>Confiança na Ofuscação ou Criptografia de Entradas Relevantes para Segurança sem Verificação de Integridade</u>
HasMembro		650	<u>Confiando nos métodos de permissão HTTP no lado do servidor</u>
HasMembro		651	<u>Exposição da informação através do arquivo WSDL</u>
HasMembro		653	<u>Compartimentalização insuficiente</u>
HasMembro		654	<u>Dependência de um fator único em uma decisão de segurança</u>
HasMembro		655	<u>Aceitabilidade Psicológica Insuficiente</u>
HasMembro		656	<u>Confiança na segurança através da obscuridade</u>
HasMembro		657	<u>Violação de Princípios de Design Seguro</u>
HasMembro		662	<u>Sincronização incorreta</u>
HasMembro		663	<u>Uso de uma função não reentrante em um contexto concorrente</u>
HasMembro		667	<u>Bloqueio Indevido</u>
HasMembro		668	<u>Exposição de Recurso à Esfera Errada</u>
HasMembro		669	<u>Transferência de recursos incorreta entre esferas</u>
HasMembro		670	<u>Implementação de Fluxo de Controle Sempre Incorreto</u>
HasMembro		671	<u>Falta de controle de administrador sobre segurança</u>
HasMembro		672	<u>Operação em um recurso após a expiração ou liberação</u>
HasMembro		673	<u>Influência Externa da Definição da Esfera</u>
HasMembro		674	<u>Recursão Descontrolada</u>
HasMembro		676	<u>Uso de Função Potencialmente Perigosa</u>
HasMembro		682	<u>Cálculo incorreto</u>
HasMembro		691	<u>Gerenciamento insuficiente de fluxo de controle</u>
HasMembro		693	<u>Falha do Mecanismo de Proteção</u>

HasMembro		694	<u>Uso de vários recursos com identificador duplicado</u>
HasMembro		695	<u>Uso da funcionalidade de baixo nível</u>
HasMembro		696	<u>Ordem de Comportamento Incorreta</u>
HasMembro		703	<u>Verificação ou manuseio inadequado de condições excepcionais</u>
HasMembro		704	<u>Conversão ou elenco de tipo incorreto</u>
HasMembro		705	<u>Escopo do controle de controle incorreto</u>
HasMembro		706	<u>Uso de Nome ou Referência Resolvidos Incorretamente</u>
HasMembro		707	<u>Aplicação indevida de mensagem ou estrutura de dados</u>
HasMembro		708	<u>Atribuição de propriedade incorreta</u>
HasMembro		710	<u>Aderência inadequada aos padrões de codificação</u>
HasMembro		732	<u>Atribuição de Permissão Incorreta para Recurso Crítico</u>
HasMembro		749	<u>Método perigoso ou função exposta</u>
HasMembro		757	<u>Seleção de Algoritmo Menos Seguro durante a Negociação ('Downgrade de Algoritmo')</u>
HasMembro		764	<u>Vários bloqueios de um recurso crítico</u>
HasMembro		766	<u>Variável Crítica Declarada Pública</u>
HasMembro		767	<u>Acesso à variável privada crítica via método público</u>
HasMembro		769	<u>Consumo do Descritor de Arquivo Não Controlado</u>
HasMembro		770	<u>Alocação de Recursos sem Limites ou Limitação</u>
HasMembro		771	<u>Referência ausente ao recurso alocado ativo</u>
HasMembro		772	<u>Liberação ausente de recurso após a vida útil efetiva</u>
HasMembro		773	<u>Referência ausente ao descritor de arquivo ativo ou identificador</u>
HasMembro		774	<u>Alocação de descritores de arquivo ou identificadores sem limites ou</u>

			<u>limitação</u>
HasMembro	● V	780	<u>Uso do Algoritmo RSA sem OAEP</u>
HasMembro	● V	781	<u>Validação incorreta de endereço no IOCTL com código de controle de E / S de METHOD_NEITHER</u>
HasMembro	● V	782	<u>IOCTL exposto com controle de acesso insuficiente</u>
HasMembro	● V	784	<u>Confiança em cookies sem validação e verificação de integridade em uma decisão de segurança</u>
HasMembro	● V	789	<u>Alocação de Memória Descontrolada</u>
HasMembro	● B	798	<u>Uso de credenciais codificadas</u>
HasMembro	● C	799	<u>Controle inadequado de frequência de interação</u>
HasMembro	● B	804	<u>CAPTCHA adivinhado</u>
HasMembro	● B	807	<u>Confiança em entradas não confiáveis em uma decisão de segurança</u>
HasMembro	● C	862	<u>Autorização ausente</u>
HasMembro	● C	863	<u>Autorização incorreta</u>
HasMembro	● C	912	<u>Funcionalidade oculta</u>
HasMembro	● C	913	<u>Controle impróprio de recursos de código gerenciados dinamicamente</u>
HasMembro	● B	914	<u>Controle impróprio de variáveis dinamicamente identificadas</u>
HasMembro	● B	915	<u>Modificação incorretamente controlada de atributos de objetos determinados dinamicamente</u>
HasMembro	● B	916	<u>Uso de Hash de Senha com Esforço Computacional Insuficiente</u>
HasMembro	● B	917	<u>Neutralização indevida de elementos especiais usados em uma declaração de linguagem de expressão ('Expression Language Injection')</u>
HasMembro	● B	918	<u>Falsificação de Solicitação do Lado do Servidor (SSRF)</u>
HasMembro	● B	920	<u>Restrição Indevida do Consumo de Energia</u>
HasMembro	● B	921	<u>Armazenamento de Dados Sensíveis em um Mecanismo sem Controle de</u>

			<u>Acesso</u>
HasMembro	(C)	922	<u>Armazenamento Inseguro de Informações Confidenciais</u>
HasMembro	(C)	923	<u>Restrição Indevida do Canal de Comunicação para Endpoints Pretendidos</u>
HasMembro	(C)	924	<u>Aplicação indevida da integridade da mensagem durante a transmissão em um canal de comunicação</u>
HasMembro	(V)	925	<u>Verificação indevida da intenção pelo receptor de transmissão</u>
HasMembro	(V)	926	<u>Exportação imprópria de componentes de aplicativos Android</u>
HasMembro	(V)	927	<u>Uso de Intenção Implícita para Comunicação Sensível</u>
HasMembro	(B)	940	<u>Verificação imprópria da fonte de um canal de comunicação</u>
HasMembro	(B)	941	<u>Destino especificado incorretamente em um canal de comunicação</u>
HasMembro	(V)	942	<u>Whitelist de domínio cruzado excessivamente permissivo</u>
HasMembro	(V)	1004	<u>Cookie sensível sem sinalizador 'HttpOnly'</u>
HasMembro	(B)	1007	<u>Distorção Visual Insuficiente de Homoglifos Apresentados ao Usuário</u>
HasMembro	(V)	1022	<u>Uso do link da Web para o destino não confiável com o acesso window.opener</u>
HasMembro	(B)	1037	<u>Remoção de otimização de processador ou modificação de código crítico de segurança</u>
HasMembro	(C)	1038	<u>Otimizações automatizadas inseguras</u>
HasMembro	(C)	1039	<u>Mecanismo de Reconhecimento Automatizado com Detecção Inadequada ou Manipulação de Perturbações de Entrada Adversa</u>

Vulnerabilidades de codificação:

Natureza	Tipo	Identidade	Nome
----------	------	------------	------

HasMembro		5	<u>J2EE Misconfiguration: Transmissão de dados sem criptografia</u>
HasMembro		6	<u>Configuração incorreta de J2EE: comprimento de ID de sessão insuficiente</u>
HasMembro		7	<u>Configuração incorreta do J2EE: página de erro personalizada ausente</u>
HasMembro		8	<u>Configuração incorreta de J2EE: Bean de entidade declarado remoto</u>
HasMembro		9	<u>Configuração incorreta do J2EE: Permissões de acesso fracas para métodos EJB</u>
HasMembro		11	<u>Configuração incorreta do ASP.NET: Criando binário de depuração</u>
HasMembro		12	<u>Configuração incorreta do ASP.NET: página de erro personalizada ausente</u>
HasMembro		13	<u>Configuração incorreta do ASP.NET: senha no arquivo de configuração</u>
HasMembro		14	<u>Remoção de código do compilador para limpar buffers</u>
HasMembro		15	<u>Controle externo do sistema ou configuração</u>
HasMembro		20	<u>Validação de entrada incorreta</u>
HasMembro		22	<u>Limitação indevida de um nome de caminho para um diretório restrito ('Traverso de caminho')</u>
HasMembro		23	<u>Travessia de Caminho Relativo</u>
HasMembro		24	<u>Caminho Traversal: '../filedir'</u>
HasMembro		25	<u>Caminho Traversal: '/..../filedir'</u>
HasMembro		26	<u>Caminho Traversal: '/dir/..../filename'</u>
HasMembro		27	<u>Caminho Traversal: 'dir /..../filename'</u>
HasMembro		28	<u>Caminho Traversal: '.. \ filedir'</u>
HasMembro		29	<u>Caminho Traversal: '\ .. \ filename'</u>
HasMembro		30	<u>Caminho Traversal: '\ dir \ .. \ filename'</u>
HasMembro		31	<u>Caminho Traversal: 'dir \ .. \ .. \ filename'</u>

HasMembro		32	<u>Caminho Traversal: '...' (Ponto Triplo)</u>
HasMembro		33	<u>Caminho Traversal: '....' (vários pontos)</u>
HasMembro		34	<u>Caminho Traversal: '.... //'</u>
HasMembro		35	<u>Caminho Traversal: '... / ... //'</u>
HasMembro		36	<u>Travessia de caminho absoluto</u>
HasMembro		37	<u>Caminho Traversal: '/ absolute / pathname / here'</u>
HasMembro		38	<u>Caminho Traversal: '\ absolute \ pathname \ here'</u>
HasMembro		39	<u>Caminho Traversal: 'C: dirname'</u>
HasMembro		40	<u>Caminho Traversal: '\\ UNC \ share \ name \' (Compartilhamento UNC do Windows)</u>
HasMembro		41	<u>Resolução imprópria de equivalência de trajetória</u>
HasMembro		42	<u>Equivalência de caminho: 'nome do arquivo'. (Ponto de fuga)</u>
HasMembro		43	<u>Equivalência de caminho: 'filename' (Multiple Trailing Dot)</u>
HasMembro		44	<u>Equivalência de caminho: 'file.name' (ponto interno)</u>
HasMembro		45	<u>Equivalência de caminho: 'file ... name' (Multiple Internal Dot)</u>
HasMembro		46	<u>Equivalência de caminho: 'filename' (Espaço à direita)</u>
HasMembro		47	<u>Equivalência de caminho: 'filename' (Leading Space)</u>
HasMembro		48	<u>Equivalência de caminho: 'file name' (espaço em branco interno)</u>
HasMembro		49	<u>Equivalência de caminho: 'filename /' (Barra de acompanhamento)</u>
HasMembro		50	<u>Equivalência de caminho: '// multiple / leading / slash'</u>
HasMembro		51	<u>Equivalência de caminho: '/ multiple // internal / slash'</u>
HasMembro		52	<u>Equivalência de caminho: '/ multiple / trailing / slash //'</u>
HasMembro		53	<u>Equivalência de caminho: '\ multiple</u>

			<u>\internal \ backslash'</u>
HasMembro	●	54	<u>Equivalência de caminho: 'filedir' (Trailing Backslash)</u>
HasMembro	●	55	<u>Equivalência de caminho: './' (Diretório de um único ponto)</u>
HasMembro	●	56	<u>Equivalência de caminho: 'filedir *' (coringa)</u>
HasMembro	●	57	<u>Equivalência de caminho: 'fakedir ../../ realdir / filename'</u>
HasMembro	●	58	<u>Equivalência de caminho: nome de arquivo do Windows 8.3</u>
HasMembro	●	59	<u>Resolução de Link Inadequada Antes do Acesso ao Arquivo ('Link Following')</u>
HasMembro	●	61	<u>Link simbólico do UNIX (Symlink) seguindo</u>
HasMembro	●	62	<u>Hard Link do UNIX</u>
HasMembro	●	65	<u>Windows Hard Link</u>
HasMembro	●	66	<u>Manipulação imprópria de nomes de arquivos que identificam recursos virtuais</u>
HasMembro	●	67	<u>Manipulação imprópria de nomes de dispositivos do Windows</u>
HasMembro	●	69	<u>Manuseio inadequado do Windows :: DATA Alternate Data Stream</u>
HasMembro	●	72	<u>Manipulação imprópria do caminho de fluxo de dados alternativo Apple HFS +</u>
HasMembro	●	73	<u>Controle Externo do Nome ou Caminho do Arquivo</u>
HasMembro	●	74	<u>Neutralização inadequada de elementos especiais na saída usada por um componente de Downstream ('Injection')</u>
HasMembro	●	75	<u>Falha na limpeza de elementos especiais em um plano diferente (injeção de elemento especial)</u>
HasMembro	●	76	<u>Neutralização indevida de elementos especiais equivalentes</u>
HasMembro	●	77	<u>Neutralização inadequada de</u>

			<u>elementos especiais usados em um comando ('Command Injection')</u>
HasMembro	Ⓑ	78	<u>Neutralização indevida de elementos especiais usados em um comando do sistema operacional ('injeção de comando do sistema operacional')</u>
HasMembro	Ⓑ	79	<u>Neutralização incorreta de entrada durante a geração de páginas da Web ('Cross-site Scripting')</u>
HasMembro	ⓧ	80	<u>Neutralização indevida de tags HTML relacionadas a scripts em uma página da Web (XSS básico)</u>
HasMembro	ⓧ	81	<u>Neutralização incorreta do script em uma página da Web de mensagem de erro</u>
HasMembro	ⓧ	82	<u>Neutralização indevida de script em atributos de tags IMG em uma página da Web</u>
HasMembro	ⓧ	83	<u>Neutralização incorreta de script em atributos em uma página da Web</u>
HasMembro	ⓧ	84	<u>Neutralização inadequada de esquemas de URI codificados em uma página da Web</u>
HasMembro	ⓧ	85	<u>Manipulações XSS de caracteres duplos</u>
HasMembro	ⓧ	86	<u>Neutralização incorreta de caracteres inválidos em identificadores em páginas da Web</u>
HasMembro	ⓧ	87	<u>Neutralização indevida de sintaxe XSS alternativa</u>
HasMembro	Ⓑ	88	<u>Injeção ou modificação de argumento</u>
HasMembro	Ⓑ	89	<u>Neutralização indevida de elementos especiais usados em um comando SQL ('SQL Injection')</u>
HasMembro	Ⓑ	90	<u>Neutralização indevida de elementos especiais usados em uma consulta LDAP ('LDAP Injection')</u>
HasMembro	Ⓑ	91	<u>Injeção de XML (também conhecido como Injeção XPath Cega)</u>
HasMembro	Ⓑ	93	<u>Neutralização Incorreta das</u>

			<u>Sequências CRLF ('CRLF Injection')</u>
HasMembro	(C)	94	<u>Controle indevido de geração de código ('Code Injection')</u>
HasMembro	(B)	95	<u>Neutralização Indevida de Diretivas em Código Avaliada Dinamicamente ('Injeção de Eval')</u>
HasMembro	(B)	96	<u>Neutralização indevida de diretivas em código salvo estaticamente ('Injeção de código estático')</u>
HasMembro	(V)	97	<u>Neutralização incorreta de inclusões do lado do servidor (SSI) em uma página da Web</u>
HasMembro	(B)	98	<u>Controle inadequado de nome de arquivo para incluir / exigir declaração no programa PHP ('PHP Remote File Inclusion')</u>
HasMembro	(B)	99	<u>Controle impróprio de identificadores de recursos ('Injeção de recursos')</u>
HasMembro	(V)	102	<u>Struts: formulários de validação duplicados</u>
HasMembro	(V)	103	<u>Struts: Validate incompleto ()</u> <u>Definição do método</u>
HasMembro	(V)	104	<u>Struts: o bean de formulário não estende a classe de validação</u>
HasMembro	(V)	105	<u>Struts: campo de formulário sem validador</u>
HasMembro	(V)	106	<u>Struts: Plug-in Framework não está em uso</u>
HasMembro	(V)	107	<u>Struts: Formulário de validação não utilizado</u>
HasMembro	(V)	108	<u>Struts: formulário de ação não validado</u>
HasMembro	(V)	109	<u>Struts: validador desativado</u>
HasMembro	(V)	110	<u>Struts: Validator sem campo de formulário</u>
HasMembro	(B)	111	<u>Uso direto de JNI inseguro</u>
HasMembro	(B)	112	<u>Validação de XML ausente</u>
HasMembro	(B)	113	<u>Neutralização incorreta de seqüências CRLF em cabeçalhos HTTP ('divisão de resposta HTTP')</u>

HasMembro	B	114	<u>Controlo do processo</u>
HasMembro	B	115	<u>Interpretação errada da entrada</u>
HasMembro	C	116	<u>Codificação imprópria ou escape de saída</u>
HasMembro	B	117	<u>Neutralização de saída imprópria para logs</u>
HasMembro	C	118	<u>Acesso incorreto do recurso indexável ('Erro de intervalo')</u>
HasMembro	C	119	<u>Restrição indevida de operações dentro dos limites de um buffer de memória</u>
HasMembro	B	120	<u>Cópia de Buffer sem Verificação do Tamanho da Entrada ('Estouro de Buffer Clássico')</u>
HasMembro	V	121	<u>Estouro de buffer com base em pilha</u>
HasMembro	V	122	<u>Excesso de buffer com base em heap</u>
HasMembro	B	123	<u>Escreva-que-onde condição</u>
HasMembro	B	124	<u>Underwrite de buffer ('Buffer Underflow')</u>
HasMembro	B	125	<u>Leitura fora dos limites</u>
HasMembro	V	126	<u>Buffer Over-read</u>
HasMembro	V	127	<u>Buffer Under-read</u>
HasMembro	B	128	<u>Erro de contorno</u>
HasMembro	B	129	<u>Validação imprópria do índice de matriz</u>
HasMembro	B	130	<u>Manipulação imprópria da inconsistência de parâmetro de comprimento</u>
HasMembro	B	131	<u>Cálculo incorreto do tamanho do buffer</u>
HasMembro	B	134	<u>Uso de String de Formato Controlado Externamente</u>
HasMembro	B	135	<u>Cálculo incorreto do comprimento de seqüência de caracteres de vários bytes</u>
HasMembro	C	138	<u>Neutralização indevida de elementos especiais</u>
HasMembro	B	140	<u>Neutralização Indevida de Delimitadores</u>
HasMembro	V	141	<u>Neutralização indevida de</u>

			<u>delimitadores de parâmetro / argumento</u>
HasMembro	● V	142	<u>Neutralização Inadequada de Delimitadores de Valor</u>
HasMembro	● V	143	<u>Neutralização indevida de Delimitadores de Registro</u>
HasMembro	● V	144	<u>Neutralização Inadequada de Delimitadores de Linhas</u>
HasMembro	● V	145	<u>Neutralização inadequada de Delimitadores de Seção</u>
HasMembro	● V	146	<u>Neutralização imprópria de Delimitadores de Expressão / Comando</u>
HasMembro	● V	147	<u>Neutralização inadequada de terminadores de entrada</u>
HasMembro	● V	148	<u>Neutralização inadequada de líderes de entrada</u>
HasMembro	● V	149	<u>Neutralização Incorreta da Sintaxe de Citação</u>
HasMembro	● V	150	<u>Neutralização indevida de seqüências de escape, meta ou controle</u>
HasMembro	● V	151	<u>Neutralização Inadequada de Delimitadores de Comentário</u>
HasMembro	● V	152	<u>Neutralização inadequada de símbolos de macro</u>
HasMembro	● V	153	<u>Neutralização inadequada de caracteres de substituição</u>
HasMembro	● V	154	<u>Neutralização indevida de delimitadores de nomes de variáveis</u>
HasMembro	● V	155	<u>Neutralização indevida de curingas ou símbolos correspondentes</u>
HasMembro	● V	156	<u>Neutralização inadequada do espaço em branco</u>
HasMembro	● V	157	<u>Falha em Sanitizar Delimitadores Emparelhados</u>
HasMembro	● V	158	<u>Neutralização imprópria de bytes nulos ou caracteres NUL</u>
HasMembro	● C	159	<u>Falha na limpeza do elemento especial</u>
HasMembro	● V	160	<u>Neutralização indevida de elementos</u>

			<u>especiais importantes</u>
HasMembro	ⓧ	161	<u>Neutralização inadequada de vários elementos especiais importantes</u>
HasMembro	ⓧ	162	<u>Neutralização indevida de elementos especiais de arrasto</u>
HasMembro	ⓧ	163	<u>Neutralização incorreta de vários elementos especiais de arrasto</u>
HasMembro	ⓧ	164	<u>Neutralização inadequada de elementos especiais internos</u>
HasMembro	ⓧ	165	<u>Neutralização incorreta de vários elementos especiais internos</u>
HasMembro	Ⓑ	166	<u>Manipulação imprópria de elemento especial ausente</u>
HasMembro	Ⓑ	167	<u>Manipulação imprópria do elemento especial adicional</u>
HasMembro	Ⓑ	168	<u>Manipulação imprópria de elementos especiais inconsistentes</u>
HasMembro	Ⓑ	170	<u>Rescisão Nula Inadequada</u>
HasMembro	Ⓒ	172	<u>Erro de codificação</u>
HasMembro	ⓧ	173	<u>Manipulação imprópria de codificação alternativa</u>
HasMembro	ⓧ	174	<u>Decodificação Dupla dos Mesmos Dados</u>
HasMembro	ⓧ	175	<u>Manipulação imprópria de codificação mista</u>
HasMembro	ⓧ	176	<u>Manipulação imprópria de codificação Unicode</u>
HasMembro	ⓧ	177	<u>Manipulação imprópria de codificação de URL (codificação hexadecimal)</u>
HasMembro	Ⓑ	178	<u>Manipulação imprópria da sensibilidade do caso</u>
HasMembro	Ⓑ	179	<u>Ordem de Comportamento Incorreta: Validação Antecipada</u>
HasMembro	Ⓑ	180	<u>Ordem de comportamento incorreta: valide antes de canonizar</u>
HasMembro	Ⓑ	181	<u>Ordem de Comportamento Incorreta: Validar Antes de Filtrar</u>
HasMembro	Ⓑ	182	<u>Colapso de dados em valor inseguro</u>
HasMembro	Ⓑ	183	<u>Whitelist permissiva</u>
HasMembro	Ⓑ	184	<u>Lista negra incompleta</u>

HasMembro		185	<u>Expressão Regular Incorreta</u>
HasMembro		186	<u>Expressão Regular excessivamente restritiva</u>
HasMembro		187	<u>Comparação Parcial de Cadeia</u>
HasMembro		188	<u>Confiança no layout de dados / memória</u>
HasMembro		190	<u>Excesso de Inteiro ou Envolvente</u>
HasMembro		191	<u>Inferior Inteiro (Wrap ou Wraparound)</u>
HasMembro		192	<u>Erro de coerção de inteiro</u>
HasMembro		193	<u>Erro off-by-one</u>
HasMembro		194	<u>Extensão de sinal inesperada</u>
HasMembro		195	<u>Assinado para erro de conversão não assinado</u>
HasMembro		196	<u>Não assinado para o erro de conversão assinado</u>
HasMembro		197	<u>Erro de truncamento numérico</u>
HasMembro		198	<u>Uso de pedidos incorretos de bytes</u>
HasMembro		200	<u>Exposição de informação</u>
HasMembro		201	<u>Exposição de informação através de dados enviados</u>
HasMembro		202	<u>Exposição de dados confidenciais por meio de consultas de dados</u>
HasMembro		203	<u>Exposição da informação através da discrepância</u>
HasMembro		204	<u>Exposição da informação da discrepância da resposta</u>
HasMembro		205	<u>Exposição da informação através da discrepância comportamental</u>
HasMembro		206	<u>Exposição da informação do estado interno através da inconsistência comportamental</u>
HasMembro		207	<u>Exposição da informação através de uma inconsistência comportamental externa</u>
HasMembro		208	<u>Exposição da informação através da discrepância de tempo</u>
HasMembro		209	<u>Exposição da informação através de uma mensagem de erro</u>
HasMembro		210	<u>Exposição da informação através da</u>

			<u>mensagem de erro autogerada</u>
HasMembro	(B)	211	<u>Exposição da informação através da mensagem de erro gerada externamente</u>
HasMembro	(B)	212	<u>Remoção transfronteiriça imprópria de dados confidenciais</u>
HasMembro	(B)	213	<u>Exposição intencional de informações</u>
HasMembro	(V)	214	<u>Exposição da informação através do ambiente do processo</u>
HasMembro	(V)	215	<u>Exposição de informações através de informações de depuração</u>
HasMembro	(C)	216	<u>Eros de contenção (erros de contêiner)</u>
HasMembro	(V)	219	<u>Dados confidenciais na raiz da Web</u>
HasMembro	(C)	221	<u>Perda de informação ou omissão</u>
HasMembro	(B)	222	<u>Truncamento de informações relevantes para segurança</u>
HasMembro	(B)	223	<u>Omissão de informações relevantes para a segurança</u>
HasMembro	(B)	224	<u>Informações relevantes sobre segurança obscuras por nome alternativo</u>
HasMembro	(B)	226	<u>Informações confidenciais não esclarecidas antes do lançamento</u>
HasMembro	(C)	228	<u>Manipulação imprópria da estrutura sintaticamente inválida</u>
HasMembro	(B)	229	<u>Manipulação imprópria de valores</u>
HasMembro	(V)	230	<u>Manipulação imprópria de valores ausentes</u>
HasMembro	(V)	231	<u>Manipulação imprópria de valores extras</u>
HasMembro	(V)	232	<u>Manipulação imprópria de valores indefinidos</u>
HasMembro	(B)	233	<u>Manipulação imprópria de parâmetros</u>
HasMembro	(V)	234	<u>Falha ao lidar com o parâmetro ausente</u>
HasMembro	(V)	235	<u>Manipulação imprópria de parâmetros extras</u>
HasMembro	(V)	236	<u>Manipulação indevida de parâmetros</u>

			<u>indefinidos</u>
HasMembro	● V	238	<u>Manipulação imprópria de elementos estruturais incompletos</u>
HasMembro	● V	239	<u>Falha ao lidar com elemento incompleto</u>
HasMembro	● B	240	<u>Manipulação imprópria de elementos estruturais inconsistentes</u>
HasMembro	● B	241	<u>Manipulação imprópria do tipo de dados inesperados</u>
HasMembro	● B	242	<u>Uso da Função Inerentemente Perigosa</u>
HasMembro	● V	243	<u>Criação de Chroot Jail Without Changing Working Directory</u>
HasMembro	● V	244	<u>Limpeza indevida de memória heap antes da liberação ('inspeção de heap')</u>
HasMembro	● V	245	<u>Boas Práticas do J2EE: Gerenciamento Direto de Conexões</u>
HasMembro	● V	246	<u>Boas Práticas do J2EE: Uso Direto dos Soquetes</u>
HasMembro	● B	248	<u>Exceção não capturada</u>
HasMembro	● C	250	<u>Execução com Privilégios Desnecessários</u>
HasMembro	● B	252	<u>Valor de Retorno Não Verificado</u>
HasMembro	● B	253	<u>Verificação incorreta do valor de retorno da função</u>
HasMembro	● V	258	<u>Senha vazia no arquivo de configuração</u>
HasMembro	● B	259	<u>Uso de senha codificada</u>
HasMembro	● V	260	<u>Senha no arquivo de configuração</u>
HasMembro	● B	266	<u>Atribuição de Privilégio Incorreta</u>
HasMembro	● B	267	<u>Privilégio Definido com Ações Não Seguras</u>
HasMembro	● B	268	<u>Encadeamento de Privilégios</u>
HasMembro	● C	269	<u>Gerenciamento impróprio de privilégios</u>
HasMembro	● B	270	<u>Erro de comutação de contexto de privilégio</u>
HasMembro	● C	271	<u>Erros de queda / redução de privilégios</u>

HasMembro		272	<u>Violação pelo Menor Privilégio</u>
HasMembro		273	<u>Verificação imprópria para privilégios descartados</u>
HasMembro		274	<u>Manipulação imprópria de privilégios insuficientes</u>
HasMembro		276	<u>Permissões padrão incorretas</u>
HasMembro		277	<u>Permissões herdadas inseguras</u>
HasMembro		279	<u>Permissões atribuídas à execução incorreta</u>
HasMembro		280	<u>Manipulação indevida de permissões ou privilégios insuficientes</u>
HasMembro		281	<u>Preservação indevida de permissões</u>
HasMembro		284	<u>Controle de Acesso Impróprio</u>
HasMembro		285	<u>Autorização Indevida</u>
HasMembro		286	<u>Gerenciamento incorreto de usuários</u>
HasMembro		287	<u>Autenticação Inadequada</u>
HasMembro		289	<u>Bypass de Autenticação por Nome Alternativo</u>
HasMembro		290	<u>Bypass de Autenticação por Spoofing</u>
HasMembro		295	<u>Validação incorreta de certificado</u>
HasMembro		296	<u>Seguimento impróprio da cadeia de confiança de um certificado</u>
HasMembro		297	<u>Validação imprópria de certificado com incompatibilidade de host</u>
HasMembro		298	<u>Validação imprópria da validade do certificado</u>
HasMembro		299	<u>Verificação indevida de revogação de certificado</u>
HasMembro		302	<u>Bypass de Autenticação por Dados Assumidos-Imutáveis</u>
HasMembro		303	<u>Implementação Incorreta do Algoritmo de Autenticação</u>
HasMembro		304	<u>Etapa crítica ausente na autenticação</u>
HasMembro		305	<u>Bypass de Autenticação por Fraqueza Primária</u>
HasMembro		318	<u>Armazenamento em texto não criptografado de informações confidenciais no executável</u>
HasMembro		325	<u>Etapa criptográfica necessária</u>

			<u>ausente</u>
HasMembro	V	329	<u>Não usando um Random IV com o modo CBC</u>
HasMembro	C	330	<u>Uso de valores aleatórios insuficientes</u>
HasMembro	B	331	<u>Entropia insuficiente</u>
HasMembro	V	332	<u>Entropia insuficiente no PRNG</u>
HasMembro	V	333	<u>Manipulação indevida de entropia insuficiente no TRNG</u>
HasMembro	B	334	<u>Pequeno espaço de valores aleatórios</u>
HasMembro	B	335	<u>Uso Incorreto de Sementes no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro	B	336	<u>Mesma Semente no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro	B	337	<u>Semente Previsível no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro	B	338	<u>Uso do Gerador de Números Pseudo-Randomizados Criptograficamente Fracos (PRNG)</u>
HasMembro	B	339	<u>Espaço Pequeno de Semente no PRNG</u>
HasMembro	C	340	<u>Problemas de Previsibilidade</u>
HasMembro	B	341	<u>Previsível do estado observável</u>
HasMembro	B	342	<u>Valor Exato Previsível dos Valores Anteriores</u>
HasMembro	B	343	<u>Intervalo de valores previsíveis dos valores anteriores</u>
HasMembro	B	344	<u>Uso de valor invariante em contexto dinamicamente variável</u>
HasMembro	C	345	<u>Verificação insuficiente de autenticidade de dados</u>
HasMembro	B	346	<u>Erro de validação de origem</u>
HasMembro	B	347	<u>Verificação imprópria da assinatura criptográfica</u>
HasMembro	B	348	<u>Uso de menor fonte confiável</u>
HasMembro	B	349	<u>Aceitação de dados não confiáveis irrelevantes com dados confiáveis</u>
HasMembro	B	351	<u>Distinção de Tipo Insuficiente</u>

HasMembro		353	<u>Suporte ausente para verificação de integridade</u>
HasMembro		354	<u>Validação imprópria do valor de verificação de integridade</u>
HasMembro		356	<u>A interface do usuário do produto não avisa o usuário de ações não seguras</u>
HasMembro		357	<u>Aviso de IU insuficiente de operações perigosas</u>
HasMembro		358	<u>Verificação de segurança incorretamente implementada para padrão</u>
HasMembro		359	<u>Exposição de Informações Privadas ('Violação de Privacidade')</u>
HasMembro		360	<u>Confiança dos dados do evento do sistema</u>
HasMembro		362	<u>Execução Concorrente usando Recurso Compartilhado com Sincronização Indevida ('Condição de Corrida')</u>
HasMembro		363	<u>Condição de Corrida Habilitando Link Following</u>
HasMembro		364	<u>Condição de corrida de manipulador de sinal</u>
HasMembro		365	<u>Condição de Corrida no Switch</u>
HasMembro		366	<u>Condição de corrida dentro de um segmento</u>
HasMembro		367	<u>Tempo de verificação Tempo de uso (TOCTOU) Race Condition</u>
HasMembro		368	<u>Condição de Corrida de Comutação de Contexto</u>
HasMembro		369	<u>Dívida por zero</u>
HasMembro		370	<u>Verificação ausente da revogação de certificado após a verificação inicial</u>
HasMembro		372	<u>Distinção Incompleta do Estado Interno</u>
HasMembro		374	<u>Passando objetos mutáveis para um método não confiável</u>
HasMembro		375	<u>Retornando um objeto mutável a um chamador não confiável</u>

HasMembro		377	<u>Arquivo temporário inseguro</u>
HasMembro		378	<u>Criação de arquivo temporário com permissões inseguras</u>
HasMembro		379	<u>Criação de arquivo temporário no diretório com permissões incorretas</u>
HasMembro		382	<u>Boas Práticas do J2EE: Uso de System.exit ()</u>
HasMembro		383	<u>Boas práticas do J2EE: uso direto de threads</u>
HasMembro		384	<u>Fixação de sessão</u>
HasMembro		385	<u>Canal de temporização secreto</u>
HasMembro		386	<u>Nome simbólico não mapeando para corrigir o objeto</u>
HasMembro		390	<u>Detecção da condição de erro sem ação</u>
HasMembro		391	<u>Condição de erro não verificado</u>
HasMembro		392	<u>Relatório de falta de condição de erro</u>
HasMembro		393	<u>Retorno do Código de Status Errado</u>
HasMembro		394	<u>Código de status inesperado ou valor de retorno</u>
HasMembro		395	<u>Uso do NullPointerException Catch para detectar desreferenciamento de ponteiro NULL</u>
HasMembro		396	<u>Declaração de captura para exceção genérica</u>
HasMembro		397	<u>Declaração de lançamentos para exceção genérica</u>
HasMembro		400	<u>Consumo Descontrolado de Recursos ('Exaustão de Recursos')</u>
HasMembro		401	<u>Liberação incorreta de memória antes de remover a última referência ('Memory Leak')</u>
HasMembro		402	<u>Transmissão de recursos privados em uma nova esfera ('vazamento de recursos')</u>
HasMembro		403	<u>Exposição do descritor de arquivo à esfera de controle não intencional ('vazamento de descritor de arquivo')</u>

HasMembro		404	<u>Encerramento ou Liberação Indevida de Recursos</u>
HasMembro		405	<u>Consumo de Recursos Assimétricos (Amplificação)</u>
HasMembro		406	<u>Controle insuficiente de volume de mensagens de rede (amplificação de rede)</u>
HasMembro		407	<u>Complexidade algorítmica</u>
HasMembro		408	<u>Ordem de Comportamento Incorreta: Amplificação Antecipada</u>
HasMembro		409	<u>Manipulação imprópria de dados altamente compactados (amplificação de dados)</u>
HasMembro		410	<u>Pool de recursos insuficiente</u>
HasMembro		412	<u>Bloqueio Acessível Externamente Irrestrito</u>
HasMembro		413	<u>Bloqueio impróprio de recursos</u>
HasMembro		414	<u>Verificação de bloqueio ausente</u>
HasMembro		415	<u>Double Free</u>
HasMembro		416	<u>Use After Free</u>
HasMembro		419	<u>Canal principal desprotegido</u>
HasMembro		420	<u>Canal alternativo desprotegido</u>
HasMembro		425	<u>Solicitação Direta ('Navegação Forçada')</u>
HasMembro		426	<u>Caminho de pesquisa não confiável</u>
HasMembro		427	<u>Elemento do caminho de pesquisa descontrolada</u>
HasMembro		428	<u>Caminho ou elemento de pesquisa sem aspas</u>
HasMembro		430	<u>Implantação do manipulador errado</u>
HasMembro		431	<u>Manipulador ausente</u>
HasMembro		432	<u>Manipulador de sinal perigoso não desativado durante operações confidenciais</u>
HasMembro		433	<u>Entrega de Conteúdo Web Não Unseaded</u>
HasMembro		434	<u>Upload irrestrito de arquivo com tipo perigoso</u>
HasMembro		435	<u>Interação imprópria entre várias entidades que se comportam</u>

			<u>corretamente</u>
HasMembro	(B)	436	<u>Interpretação Conflito</u>
HasMembro	(B)	437	<u>Modelo Incompleto de Recursos de Ponto Final</u>
HasMembro	(B)	439	<u>Mudança Comportamental em Nova Versão ou Ambiente</u>
HasMembro	(B)	440	<u>Violação esperada de comportamento</u>
HasMembro	(B)	444	<u>Interpretação Inconsistente de Pedidos HTTP ('HTTP Request Smuggling')</u>
HasMembro	(B)	446	<u>Discrepância da interface do usuário para o recurso de segurança</u>
HasMembro	(B)	447	<u>Recurso não implementado ou não suportado na interface do usuário</u>
HasMembro	(B)	448	<u>Recurso Obsoleto na IU</u>
HasMembro	(B)	449	<u>A interface do usuário executa a ação errada</u>
HasMembro	(B)	450	<u>Múltiplas Interpretações da Entrada da Interface do Usuário</u>
HasMembro	(C)	451	<u>Interface do usuário (IU) Deturpação de informações críticas</u>
HasMembro	(B)	453	<u>Inicialização de Variável Padrão Insegura</u>
HasMembro	(B)	454	<u>Inicialização Externa de Variáveis Confiáveis ou Armazenamentos de Dados</u>
HasMembro	(B)	455	<u>Não-saída na inicialização com falha</u>
HasMembro	(B)	456	<u>Inicialização ausente de uma variável</u>
HasMembro	(V)	457	<u>Uso de Variável Não Inicializada</u>
HasMembro	(B)	459	<u>Limpeza Incompleta</u>
HasMembro	(V)	460	<u>Limpeza imprópria na exceção lançada</u>
HasMembro	(B)	462	<u>Chave Duplicada na Lista Associativa (Alist)</u>
HasMembro	(B)	463	<u>Exclusão da estrutura de dados Sentinel</u>
HasMembro	(B)	464	<u>Adição de estrutura de dados Sentinel</u>

HasMembro		466	<u>Retorno do valor do ponteiro fora do intervalo esperado</u>
HasMembro		467	<u>Uso de sizeof () em um tipo de ponteiro</u>
HasMembro		468	<u>Escala de Ponteiros Incorreta</u>
HasMembro		469	<u>Uso de subtração de ponteiro para determinar o tamanho</u>
HasMembro		470	<u>Uso de entrada controlada externamente para selecionar classes ou código ('Reflexão insegura')</u>
HasMembro		471	<u>Modificação de Dados Assumidos-Imutáveis (MAID)</u>
HasMembro		472	<u>Controle Externo do Parâmetro Web Assumido-Imutável</u>
HasMembro		473	<u>Modificação de Variáveis Externas do PHP</u>
HasMembro		474	<u>Uso de função com implementações inconsistentes</u>
HasMembro		475	<u>Comportamento indefinido para entrada na API</u>
HasMembro		476	<u>Desreferência do ponteiro NULL</u>
HasMembro		477	<u>Uso de Função Obsoleta</u>
HasMembro		478	<u>Caso padrão ausente na instrução de troca</u>
HasMembro		479	<u>Uso de manipulador de sinal de uma função não reentrante</u>
HasMembro		480	<u>Uso de operador incorreto</u>
HasMembro		481	<u>Atribuição em vez de comparar</u>
HasMembro		482	<u>Comparando em vez de Atribuindo</u>
HasMembro		483	<u>Delimitação de Bloco Incorreta</u>
HasMembro		484	<u>Declaração de quebra omitida no switch</u>
HasMembro		486	<u>Comparação de Classes por Nome</u>
HasMembro		487	<u>Confiança no escopo no nível do pacote</u>
HasMembro		488	<u>Exposição do Elemento de Dados à Sessão Errada</u>
HasMembro		489	<u>Código de Depuração de Sobras</u>
HasMembro		491	<u>Método público cloneable () sem</u>

			<u>final ('Object Hijack')</u>
HasMembro	● V	492	<u>Uso da Classe Interna Contendo Dados Sensíveis</u>
HasMembro	● V	493	<u>Variável pública crítica sem modificador final</u>
HasMembro	● B	494	<u>Download do código sem verificação de integridade</u>
HasMembro	● V	495	<u>Campo privado, digitado em matriz, retornado de um método público</u>
HasMembro	● V	496	<u>Dados públicos atribuídos ao campo privado digitado por matriz</u>
HasMembro	● V	497	<u>Exposição de dados do sistema a uma esfera de controle não autorizada</u>
HasMembro	● V	498	<u>Classe Clonável Contendo Informações Sensíveis</u>
HasMembro	● V	499	<u>Classe Serializável Contendo Dados Sensíveis</u>
HasMembro	● V	500	<u>Campo estático público não marcado final</u>
HasMembro	● V	502	<u>Desserialização de dados não confiáveis</u>
HasMembro	● C	506	<u>Código Malicioso Integrado</u>
HasMembro	● B	507	<u>Cavalo de Tróia</u>
HasMembro	● B	508	<u>Código mal-intencionado sem replicação</u>
HasMembro	● B	509	<u>Replicando códigos maliciosos (vírus ou worm)</u>
HasMembro	● B	510	<u>Alçapão</u>
HasMembro	● B	511	<u>Lógica / Time Bomb</u>
HasMembro	● B	512	<u>Spyware</u>
HasMembro	● C	514	<u>Canal secreto</u>
HasMembro	● B	515	<u>Canal de Armazenamento Secreto</u>
HasMembro	● V	520	<u>Configuração incorreta do .NET: uso de falsificação de identidade</u>
HasMembro	● B	521	<u>Requisitos de senha fraca</u>
HasMembro	● B	522	<u>Credenciais insuficientemente protegidas</u>
HasMembro	● V	524	<u>Exposição da informação através do cache</u>

HasMembro	V	525	<u>Exposição de informações através do cache do navegador</u>
HasMembro	V	526	<u>Exposição da informação através de variáveis ambientais</u>
HasMembro	V	532	<u>Exposição de informações através de arquivos de log</u>
HasMembro	V	535	<u>Exposição da informação através da mensagem de erro do escudo</u>
HasMembro	V	536	<u>Exposição da informação através da mensagem de erro do runtime de Servlet</u>
HasMembro	V	537	<u>Exposição de informações através da mensagem de erro do Java Runtime</u>
HasMembro	B	538	<u>Exposição de informações de arquivo e diretório</u>
HasMembro	V	539	<u>Exposição da informação através de cookies persistentes</u>
HasMembro	V	540	<u>Exposição da informação através do código fonte</u>
HasMembro	V	541	<u>Exposição da informação através do código fonte incluído</u>
HasMembro	V	543	<u>Uso do Padrão Singleton Sem Sincronização em um Contexto Multithread</u>
HasMembro	V	546	<u>Comentário Suspeito</u>
HasMembro	V	547	<u>Uso de constantes codificadas e relevantes para segurança</u>
HasMembro	V	548	<u>Exposição de informações por meio da listagem de diretório</u>
HasMembro	V	549	<u>Máscara de campo de senha ausente</u>
HasMembro	V	550	<u>Exposição da informação através da mensagem de erro do servidor</u>
HasMembro	B	551	<u>Ordem de Comportamento Incorreta: Autorização Antes da Análise e Canonização</u>
HasMembro	B	552	<u>Arquivos ou Diretórios Acessíveis a Partes Externas</u>
HasMembro	V	553	<u>Shell de Comando no Diretório Acessível Externamente</u>
HasMembro	V	554	<u>Configuração incorreta do ASP.NET:</u>

			<u>não usando o Input Validation Framework</u>
HasMembro	V	555	<u>Configuração incorreta de J2EE: Senha de texto sem formatação no arquivo de configuração</u>
HasMembro	V	556	<u>Configuração incorreta do ASP.NET: uso de representação de identidade</u>
HasMembro	V	558	<u>Uso de getlogin () no aplicativo multithread</u>
HasMembro	V	560	<u>Uso de umask () com o argumento chmod-style</u>
HasMembro	V	561	<u>Código Morto</u>
HasMembro	B	562	<u>Retorno do endereço da variável de pilha</u>
HasMembro	V	563	<u>Atribuição a variável sem uso</u>
HasMembro	V	564	<u>Injeção de SQL: Hibernate</u>
HasMembro	B	565	<u>Confiança em Cookies sem Validação e Verificação de Integridade</u>
HasMembro	V	566	<u>Bypass de Autorização Através da Chave Primária SQL Controlada pelo Usuário</u>
HasMembro	B	567	<u>Acesso não sincronizado a dados compartilhados em um contexto multithread</u>
HasMembro	V	568	<u>finalize () Método sem super.finalize ()</u>
HasMembro	V	570	<u>Expressão é sempre falsa</u>
HasMembro	V	571	<u>Expressão é sempre verdadeira</u>
HasMembro	V	572	<u>Chamar para Thread run () em vez de start ()</u>
HasMembro	C	573	<u>Seguimento indevido de especificação por chamador</u>
HasMembro	V	574	<u>Práticas ruins do EJB: uso de primitivas de sincronização</u>
HasMembro	V	575	<u>Boas Práticas do EJB: Uso do AWT Swing</u>
HasMembro	V	576	<u>Boas Práticas do EJB: Uso de Java I / O</u>
HasMembro	V	577	<u>Boas Práticas do EJB: Uso de Soquetes</u>

HasMembro		578	<u>Práticas incorretas do EJB: uso do carregador de classes</u>
HasMembro		579	<u>Práticas ruins do J2EE: objeto não serializável armazenado na sessão</u>
HasMembro		580	<u>clone () Método sem super.clone ()</u>
HasMembro		581	<u>Violação de modelo de objeto: apenas um dos iguais e Hashcode definido</u>
HasMembro		582	<u>Matriz Declarada Pública, Final e Estática</u>
HasMembro		583	<u>finalize () Método Declarado Público</u>
HasMembro		584	<u>Retornar no interior finalmente bloco</u>
HasMembro		585	<u>Bloco Sincronizado Vazio</u>
HasMembro		586	<u>Chamada explícita para finalizar ()</u>
HasMembro		587	<u>Atribuição de um endereço fixo a um ponteiro</u>
HasMembro		588	<u>Tentativa de acessar filho de um ponteiro de estrutura não</u>
HasMembro		589	<u>Chamada para API não onipresente</u>
HasMembro		590	<u>Livre de memória não no heap</u>
HasMembro		591	<u>Armazenamento de dados confidenciais em memória bloqueada incorretamente</u>
HasMembro		593	<u>Bypass de Autenticação: Objeto OpenSSL CTX Modificado Após a Criação dos Objetos SSL</u>
HasMembro		594	<u>J2EE Framework: Salvando Objetos Não Serializáveis no Disco</u>
HasMembro		595	<u>Comparação de referências de objetos em vez de conteúdo de objetos</u>
HasMembro		597	<u>Uso do Operador Errado na Comparação de Cadeias</u>
HasMembro		598	<u>Exposição de informações através de seqüências de caracteres de consulta no pedido GET</u>
HasMembro		599	<u>Validação perdida do certificado OpenSSL</u>
HasMembro		600	<u>Exceção não identificada no Servlet</u>
HasMembro		601	<u>Redirecionamento de URL para site</u>

			<u>não confiável ('Redirecionamento aberto')</u>
HasMembro	(B)	603	<u>Uso da Autenticação do Lado do Cliente</u>
HasMembro	(B)	605	<u>Múltiplas Vinculações à Mesma Porta</u>
HasMembro	(B)	606	<u>Entrada não verificada para condição de loop</u>
HasMembro	(V)	607	<u>Referências do campo final estático público objeto mutável</u>
HasMembro	(V)	608	<u>Struts: campo não privado na classe ActionForm</u>
HasMembro	(B)	609	<u>Bloqueio Duplo-verificado</u>
HasMembro	(V)	611	<u>Restrição Indevida da Referência de Entidade Externa XML ('XXE')</u>
HasMembro	(V)	612	<u>Exposição de informação através da indexação de dados privados</u>
HasMembro	(B)	613	<u>Expiração de sessão insuficiente</u>
HasMembro	(V)	614	<u>Cookie Sensível em Sessão HTTPS sem Atributo 'Seguro'</u>
HasMembro	(V)	615	<u>Exposição da informação através dos comentários</u>
HasMembro	(V)	616	<u>Identificação Incompleta de Variáveis de Arquivo Carregadas (PHP)</u>
HasMembro	(V)	617	<u>Afirmação Alcançável</u>
HasMembro	(B)	618	<u>Método ActiveX não seguro exposto</u>
HasMembro	(B)	619	<u>Cursor de banco de dados oscilante ('Injeção de cursor')</u>
HasMembro	(V)	620	<u>Alteração de senha não confirmada</u>
HasMembro	(B)	621	<u>Erro de Extração Variável</u>
HasMembro	(V)	622	<u>Validação incorreta de argumentos do gancho de função</u>
HasMembro	(V)	623	<u>Controle inseguro do ActiveX marcado como seguro para script</u>
HasMembro	(B)	624	<u>Erro de expressão regular executável</u>
HasMembro	(B)	625	<u>Expressão Regular Permissiva</u>
HasMembro	(V)	626	<u>Erro de Interação de Byte Nulo (Poison Null Byte)</u>
HasMembro	(B)	627	<u>Avaliação de Variáveis Dinâmicas</u>
HasMembro	(B)	628	<u>Chamada de Função com</u>

			<u>Argumentos Especificados Incorretamente</u>
HasMembro	(C)	636	<u>Não falhando com segurança ('Failing Open')</u>
HasMembro	(C)	637	<u>Complexidade Desnecessária no Mecanismo de Proteção (Não Usando a "Economia do Mecanismo")</u>
HasMembro	(C)	638	<u>Não usando mediação completa</u>
HasMembro	(B)	640	<u>Mecanismo de recuperação de senha fraca para senha esquecida</u>
HasMembro	(B)	641	<u>Restrição Incorreta de Nomes para Arquivos e Outros Recursos</u>
HasMembro	(C)	642	<u>Controle Externo de Dados Críticos do Estado</u>
HasMembro	(B)	643	<u>Neutralização Indevida de Dados em Expressões XPath ('XPath Injection')</u>
HasMembro	(V)	644	<u>Neutralização incorreta de cabeçalhos HTTP para sintaxe de script</u>
HasMembro	(V)	646	<u>Confiança no nome do arquivo ou na extensão do arquivo fornecido externamente</u>
HasMembro	(V)	647	<u>Uso de Caminhos de URL Não-Canônicos para Decisões de Autorização</u>
HasMembro	(B)	648	<u>Uso incorreto de APIs privilegiadas</u>
HasMembro	(B)	649	<u>Confiança na Ofuscação ou Criptografia de Entradas Relevantes para Segurança sem Verificação de Integridade</u>
HasMembro	(V)	650	<u>Confiando nos métodos de permissão HTTP no lado do servidor</u>
HasMembro	(V)	651	<u>Exposição da informação através do arquivo WSDL</u>
HasMembro	(B)	652	<u>Neutralização Indevida de Dados em Expressões XQuery ('XQuery Injection')</u>
HasMembro	(B)	653	<u>Compartimentalização insuficiente</u>
HasMembro	(B)	654	<u>Dependência de um fator único em uma decisão de segurança</u>

HasMembro	B	655	<u>Aceitabilidade Psicológica Insuficiente</u>
HasMembro	B	656	<u>Confiança na segurança através da obscuridade</u>
HasMembro	C	657	<u>Violação de Princípios de Design Seguro</u>
HasMembro	B	662	<u>Sincronização incorreta</u>
HasMembro	B	663	<u>Uso de uma função não reentrante em um contexto concorrente</u>
HasMembro	C	664	<u>Controle inadequado de um recurso por toda a sua vida</u>
HasMembro	C	665	<u>Inicialização incorreta</u>
HasMembro	B	666	<u>Operação no recurso na fase errada da vida</u>
HasMembro	B	667	<u>Bloqueio Indevido</u>
HasMembro	C	668	<u>Exposição de Recurso à Esfera Errada</u>
HasMembro	C	669	<u>Transferência de recursos incorreta entre esferas</u>
HasMembro	C	670	<u>Implementação de Fluxo de Controle Sempre Incorreto</u>
HasMembro	C	671	<u>Falta de controle de administrador sobre segurança</u>
HasMembro	B	672	<u>Operação em um recurso após a expiração ou liberação</u>
HasMembro	C	673	<u>Influência Externa da Definição da Esfera</u>
HasMembro	B	674	<u>Recursão Descontrolada</u>
HasMembro	C	675	<u>Operações duplicadas no recurso</u>
HasMembro	B	676	<u>Uso de Função Potencialmente Perigosa</u>
HasMembro	C	681	<u>Conversão incorreta entre tipos numéricos</u>
HasMembro	C	682	<u>Cálculo incorreto</u>
HasMembro	V	683	<u>Chamada de função com ordem incorreta de argumentos</u>
HasMembro	C	684	<u>Provisão Incorreta de Funcionalidade Especificada</u>
HasMembro	V	685	<u>Chamada de função com número incorreto de argumentos</u>

HasMembro		686	<u>Chamada de função com tipo de argumento incorreto</u>
HasMembro		687	<u>Chamada de função com valor de argumento especificado incorretamente</u>
HasMembro		688	<u>Chamada de função com variável incorreta ou referência como argumento</u>
HasMembro		689	<u>Condição de corrida de permissão durante a cópia de recurso</u>
HasMembro		690	<u>Valor de Retorno Não Verificado para Retenção de Ponteiro NULL</u>
HasMembro		691	<u>Gerenciamento insuficiente de fluxo de controle</u>
HasMembro		693	<u>Falha do Mecanismo de Proteção</u>
HasMembro		694	<u>Uso de vários recursos com identificador duplicado</u>
HasMembro		695	<u>Uso da funcionalidade de baixo nível</u>
HasMembro		696	<u>Ordem de Comportamento Incorreta</u>
HasMembro		697	<u>Comparação Incorreta</u>
HasMembro		698	<u>Execução após o redirecionamento (EAR)</u>
HasMembro		703	<u>Verificação ou manuseio inadequado de condições excepcionais</u>
HasMembro		704	<u>Conversão ou elenco de tipo incorreto</u>
HasMembro		705	<u>Escopo do controle de controle incorreto</u>
HasMembro		706	<u>Uso de Nome ou Referência Resolvidos Incorretamente</u>
HasMembro		707	<u>Aplicação indevida de mensagem ou estrutura de dados</u>
HasMembro		708	<u>Atribuição de propriedade incorreta</u>
HasMembro		710	<u>Aderência inadequada aos padrões de codificação</u>
HasMembro		732	<u>Atribuição de Permissão Incorreta para Recurso Crítico</u>
HasMembro		749	<u>Método perigoso ou função exposta</u>
HasMembro		754	<u>Verificação indevida de condições incomuns ou excepcionais</u>

HasMembro		755	<u>Manipulação indevida de condições excepcionais</u>
HasMembro		759	<u>Uso de um hash unidirecional sem sal</u>
HasMembro		760	<u>Uso de um hash unidirecional com um sal previsível</u>
HasMembro		761	<u>Livre de ponteiro não no início do buffer</u>
HasMembro		762	<u>Rotinas de Gerenciamento de Memória Incompatíveis</u>
HasMembro		763	<u>Liberação de ponteiro ou referência inválida</u>
HasMembro		764	<u>Vários bloqueios de um recurso crítico</u>
HasMembro		765	<u>Múltiplos Desbloqueios de um Recurso Crítico</u>
HasMembro		766	<u>Variável Crítica Declarada Pública</u>
HasMembro		767	<u>Acesso à variável privada crítica via método público</u>
HasMembro		768	<u>Avaliação incorreta de curto-circuito</u>
HasMembro		769	<u>Consumo do Descritor de Arquivo Não Controlado</u>
HasMembro		770	<u>Alocação de Recursos sem Limites ou Limitação</u>
HasMembro		771	<u>Referência ausente ao recurso alocado ativo</u>
HasMembro		772	<u>Liberação ausente de recurso após a vida útil efetiva</u>
HasMembro		773	<u>Referência ausente ao descritor de arquivo ativo ou identificador</u>
HasMembro		774	<u>Alocação de descritores de arquivo ou identificadores sem limites ou limitação</u>
HasMembro		775	<u>Liberação ausente do descritor de arquivo ou do identificador após a vida útil</u>
HasMembro		776	<u>Restrição Indevida de Referências de Entidade Recursiva em DTDs ('Expansão de Entidade XML')</u>
HasMembro		777	<u>Expressão Regular sem Âncoras</u>

HasMembro	V	780	<u>Uso do Algoritmo RSA sem OAEP</u>
HasMembro	V	781	<u>Validação incorreta de endereço no IOCTL com código de controle de E / S de METHOD NEITHER</u>
HasMembro	V	782	<u>IOCTL exposto com controle de acesso insuficiente</u>
HasMembro	V	783	<u>Erro de lógica de precedência do operador</u>
HasMembro	V	784	<u>Confiança em cookies sem validação e verificação de integridade em uma decisão de segurança</u>
HasMembro	V	785	<u>Uso da Função de Manipulação de Caminho sem o Buffer de Tamanho Máximo</u>
HasMembro	V	789	<u>Alocação de Memória Descontrolada</u>
HasMembro	C	790	<u>Filtragem Incorreta de Elementos Especiais</u>
HasMembro	B	791	<u>Filtragem Incompleta de Elementos Especiais</u>
HasMembro	V	792	<u>Filtragem Incompleta de uma ou mais instâncias de elementos especiais</u>
HasMembro	V	793	<u>Filtrando apenas uma instância de um elemento especial</u>
HasMembro	V	794	<u>Filtragem Incompleta de Múltiplas Instâncias de Elementos Especiais</u>
HasMembro	B	795	<u>Filtrando somente elementos especiais em um local especificado</u>
HasMembro	V	796	<u>Filtrando somente elementos especiais em relação a um marcador</u>
HasMembro	V	797	<u>Filtrando apenas elementos especiais em uma posição absoluta</u>
HasMembro	C	799	<u>Controle inadequado de frequência de interação</u>
HasMembro	B	804	<u>CAPTCHA adivinhado</u>
HasMembro	B	805	<u>Acesso de Buffer com Valor de Comprimento Incorreto</u>
HasMembro	V	806	<u>Acesso ao buffer usando o tamanho do buffer de origem</u>
HasMembro	B	807	<u>Confiança em entradas não</u>

			<u>confiáveis em uma decisão de segurança</u>
HasMembro	(B)	827	<u>Controle indevido da definição do tipo de documento</u>
HasMembro	(C)	829	<u>Inclusão de funcionalidade da esfera de controle não confiável</u>
HasMembro	(B)	830	<u>Inclusão de funcionalidade da Web de uma fonte não confiável</u>
HasMembro	(B)	836	<u>Uso de hash de senha em vez de senha para autenticação</u>
HasMembro	(B)	841	<u>Aplicação indevida do fluxo de trabalho comportamental</u>
HasMembro	(B)	842	<u>Posicionamento do usuário em grupo incorreto</u>
HasMembro	(B)	843	<u>Acesso do recurso usando o tipo incompatível ('Type Confusion')</u>
HasMembro	(C)	862	<u>Autorização ausente</u>
HasMembro	(C)	863	<u>Autorização incorreta</u>
HasMembro	(B)	908	<u>Uso de recurso não inicializado</u>
HasMembro	(B)	909	<u>Inicialização ausente do recurso</u>
HasMembro	(B)	910	<u>Uso do Descritor de Arquivo Expirado</u>
HasMembro	(B)	911	<u>Atualização incorreta da contagem de referência</u>
HasMembro	(C)	912	<u>Funcionalidade oculta</u>
HasMembro	(C)	913	<u>Controle impróprio de recursos de código gerenciados dinamicamente</u>
HasMembro	(B)	914	<u>Controle impróprio de variáveis dinamicamente identificadas</u>
HasMembro	(B)	915	<u>Modificação incorretamente controlada de atributos de objetos determinados dinamicamente</u>
HasMembro	(B)	917	<u>Neutralização indevida de elementos especiais usados em uma declaração de linguagem de expressão ('Expression Language Injection')</u>
HasMembro	(B)	918	<u>Falsificação de Solicitação do Lado do Servidor (SSRF)</u>
HasMembro	(C)	922	<u>Armazenamento Inseguro de Informações Confidenciais</u>
HasMembro	(B)	939	<u>Autorização incorreta no</u>

			<u>manipulador para esquema de URL personalizado</u>
HasMembro	(B)	940	<u>Verificação imprópria da fonte de um canal de comunicação</u>
HasMembro	(B)	941	<u>Destino especificado incorretamente em um canal de comunicação</u>
HasMembro	(V)	942	<u>Whitelist de domínio cruzado excessivamente permissivo</u>
HasMembro	(C)	943	<u>Neutralização indevida de elementos especiais na lógica de consulta de dados</u>
HasMembro	(V)	1004	<u>Cookie sensível sem sinalizador 'HttpOnly'</u>
HasMembro	(B)	1007	<u>Distorção Visual Insuficiente de Homoglifos Apresentados ao Usuário</u>
HasMembro	(B)	1021	<u>Restrição Incorreta de Camadas ou Quadros de UI Renderizados</u>
HasMembro	(V)	1022	<u>Uso do link da Web para o destino não confiável com o acesso window.opener</u>
HasMembro	(B)	1023	<u>Comparação Incompleta com Fatores Perdidos</u>
HasMembro	(B)	1024	<u>Comparação de Tipos Incompatíveis</u>
HasMembro	(B)	1025	<u>Comparação Usando Fatores Errados</u>

As vulnerabilidades de configuração são:

Natureza	Tipo	Identidade	Nome
Membro de	(V)	635	<u>Pontos Fracos Originalmente Usados pelo NVD de 2008 a 2016</u>
Membro de	(V)	699	<u>Conceitos de desenvolvimento</u>
Membro de	(C)	933	<u>OWASP Top Ten 2013 Categoria A5 - Configuração Incorreta de Segurança</u>
Membro de	(V)	1003	<u>Pontos fracos para o mapeamento simplificado de vulnerabilidades publicadas</u>
Membro de	(C)	1032	<u>OWASP Top Ten 2017 Categoria A6 - Configuração Incorreta de Segurança</u>
HasMembro	(C)	4	<u>Problemas ambientais do J2EE</u>
HasMembro	(C)	519	<u>Problemas de ambiente .NET</u>

As vulnerabilidades de codificação são:

Natureza	Tipo	Identidade	Nome
HasMembro	V	5	<u>J2EE Misconfiguration: Transmissão de dados sem criptografia</u>
HasMembro	V	6	<u>Configuração incorreta de J2EE: comprimento de ID de sessão insuficiente</u>
HasMembro	V	7	<u>Configuração incorreta do J2EE: página de erro personalizada ausente</u>
HasMembro	V	8	<u>Configuração incorreta de J2EE: Bean de entidade declarado remoto</u>
HasMembro	V	9	<u>Configuração incorreta do J2EE: Permissões de acesso fracas para métodos EJB</u>
HasMembro	V	11	<u>Configuração incorreta do ASP.NET: Criando binário de depuração</u>
HasMembro	V	12	<u>Configuração incorreta do ASP.NET: página de erro personalizada ausente</u>
HasMembro	V	13	<u>Configuração incorreta do ASP.NET: senha no arquivo de configuração</u>
HasMembro	V	14	<u>Remoção de código do compilador para limpar buffers</u>
HasMembro	B	15	<u>Controle externo do sistema ou configuração</u>
HasMembro	C	20	<u>Validação de entrada incorreta</u>
HasMembro	C	22	<u>Limitação indevida de um nome de caminho para um diretório restrito ('Traversal de caminho')</u>
HasMembro	B	23	<u>Travessia de Caminho Relativo</u>

HasMembro		24	<u>Caminho Traversal: '../filedir'</u>
HasMembro		25	<u>Caminho Traversal: '/../filedir'</u>
HasMembro		26	<u>Caminho Traversal: '/dir/..filename'</u>
HasMembro		27	<u>Caminho Traversal: 'dir /.../filename'</u>
HasMembro		28	<u>Caminho Traversal: '.. \ filedir'</u>
HasMembro		29	<u>Caminho Traversal: '\ .. \ filename'</u>
HasMembro		30	<u>Caminho Traversal: '\ dir \ .. \ filename'</u>
HasMembro		31	<u>Caminho Traversal: 'dir \ .. \ .. \ filename'</u>
HasMembro		32	<u>Caminho Traversal: '...' (Ponto Triplo)</u>
HasMembro		33	<u>Caminho Traversal: '....' (vários pontos)</u>
HasMembro		34	<u>Caminho Traversal: '.... //'</u>
HasMembro		35	<u>Caminho Traversal: '... / ... //'</u>
HasMembro		36	<u>Travessia de caminho absoluto</u>
HasMembro		37	<u>Caminho Traversal: '/ absolute / pathname / here'</u>
HasMembro		38	<u>Caminho Traversal: '\ absolute \ pathname \ here'</u>
HasMembro		39	<u>Caminho Traversal: 'C: dirname'</u>
HasMembro		40	<u>Caminho Traversal: '\\ UNC \ share \ name \' (Compartilhamento UNC do Windows)</u>
HasMembro		41	<u>Resolução imprópria de equivalência de trajetória</u>
HasMembro		42	<u>Equivalência de caminho: 'nome do</u>

			<u>arquivo'. (Ponto de fuga)</u>
HasMembro	ⓧ	43	<u>Equivalência de caminho: 'filename' (Multiple Trailing Dot)</u>
HasMembro	ⓧ	44	<u>Equivalência de caminho: 'file.name' (ponto interno)</u>
HasMembro	ⓧ	45	<u>Equivalência de caminho: 'file ... name' (Multiple Internal Dot)</u>
HasMembro	ⓧ	46	<u>Equivalência de caminho: 'filename' (Espaço à direita)</u>
HasMembro	ⓧ	47	<u>Equivalência de caminho: 'filename' (Leading Space)</u>
HasMembro	ⓧ	48	<u>Equivalência de caminho: 'file name' (espaço em branco interno)</u>
HasMembro	ⓧ	49	<u>Equivalência de caminho: 'filename /' (Barra de acompanhamento)</u>
HasMembro	ⓧ	50	<u>Equivalência de caminho: '// multiple / leading / slash'</u>
HasMembro	ⓧ	51	<u>Equivalência de caminho: '/ multiple // internal / slash'</u>
HasMembro	ⓧ	52	<u>Equivalência de caminho: '/ multiple / trailing / slash //'</u>
HasMembro	ⓧ	53	<u>Equivalência de caminho: '\ multiple \\ internal \ backslash'</u>
HasMembro	ⓧ	54	<u>Equivalência de caminho: 'filedir' (Trailing Backslash)</u>
HasMembro	ⓧ	55	<u>Equivalência de caminho: './' (Diretório de um único ponto)</u>
HasMembro	ⓧ	56	<u>Equivalência de caminho: 'filedir *' (coringa)</u>
HasMembro	ⓧ	57	<u>Equivalência de caminho: 'fakedir</u>

			<u>../ realdir / filename'</u>
HasMembro	● V	58	<u>Equivalência de caminho: nome de arquivo do Windows 8.3</u>
HasMembro	● B	59	<u>Resolução de Link Inadequada Antes do Acesso ao Arquivo ('Link Following')</u>
HasMembro	● ●	61	<u>Link simbólico do UNIX (Symlink) seguindo</u>
HasMembro	● V	62	<u>Hard Link do UNIX</u>
HasMembro	● V	65	<u>Windows Hard Link</u>
HasMembro	● B	66	<u>Manipulação imprópria de nomes de arquivos que identificam recursos virtuais</u>
HasMembro	● V	67	<u>Manipulação imprópria de nomes de dispositivos do Windows</u>
HasMembro	● V	69	<u>Manuseio inadequado do Windows :: DATA Alternate Data Stream</u>
HasMembro	● V	72	<u>Manipulação imprópria do caminho de fluxo de dados alternativo Apple HFS +</u>
HasMembro	● C	73	<u>Controle Externo do Nome ou Caminho do Arquivo</u>
HasMembro	● C	74	<u>Neutralização indevida de elementos especiais na saída usada por um componente a jusante ('Injection')</u>
HasMembro	● C	75	<u>Falha na limpeza de elementos especiais em um plano diferente (injeção de elemento especial)</u>
HasMembro	● B	76	<u>Neutralização indevida de elementos especiais equivalentes</u>
HasMembro	● C	77	<u>Neutralização inadequada de</u>

			<u>elementos especiais usados em um comando ('Command Injection')</u>
HasMembro	Ⓑ	78	<u>Neutralização indevida de elementos especiais usados em um comando do sistema operacional ('injeção de comando do sistema operacional')</u>
HasMembro	Ⓑ	79	<u>Neutralização incorreta de entrada durante a geração de páginas da Web ('Cross-site Scripting')</u>
HasMembro	ⓧ	80	<u>Neutralização indevida de tags HTML relacionadas a scripts em uma página da Web (XSS básico)</u>
HasMembro	ⓧ	81	<u>Neutralização incorreta do script em uma página da Web de mensagem de erro</u>
HasMembro	ⓧ	82	<u>Neutralização indevida de script em atributos de tags IMG em uma página da Web</u>
HasMembro	ⓧ	83	<u>Neutralização incorreta de script em atributos em uma página da Web</u>
HasMembro	ⓧ	84	<u>Neutralização inadequada de esquemas de URI codificados em uma página da Web</u>
HasMembro	ⓧ	85	<u>Manipulações XSS de caracteres duplos</u>
HasMembro	ⓧ	86	<u>Neutralização incorreta de caracteres inválidos em identificadores em páginas da Web</u>
HasMembro	ⓧ	87	<u>Neutralização indevida de sintaxe XSS alternativa</u>
HasMembro	Ⓑ	88	<u>Injeção ou modificação de argumento</u>

HasMembro		89	<u>Neutralização inadequada de elementos especiais usados em um comando SQL ('SQL Injection')</u>
HasMembro		90	<u>Neutralização indevida de elementos especiais usados em uma consulta LDAP ('LDAP Injection')</u>
HasMembro		91	<u>Injeção de XML (também conhecido como Injeção XPath Cega)</u>
HasMembro		93	<u>Neutralização Incorreta das Sequências CRLF ('CRLF Injection')</u>
HasMembro		94	<u>Controle indevido de geração de código ('Code Injection')</u>
HasMembro		95	<u>Neutralização Indevida de Diretivas em Código Avaliada Dinamicamente ('Injeção de Eval')</u>
HasMembro		96	<u>Neutralização indevida de diretivas em código salvo estaticamente ('Injeção de código estático')</u>
HasMembro		97	<u>Neutralização indevida de inclusões do lado do servidor (SSI) em uma página da Web</u>
HasMembro		98	<u>Controle inadequado de nome de arquivo para incluir / exigir declaração no programa PHP ('PHP Remote File Inclusion')</u>
HasMembro		99	<u>Controle impróprio de identificadores de recursos ('Injeção de recursos')</u>
HasMembro		102	<u>Struts: formulários de validação duplicados</u>
HasMembro		103	<u>Struts: Validate incompleto () Definição do método</u>
HasMembro		104	<u>Struts: o bean de formulário não</u>

			<u>estende a classe de validação</u>
HasMembro	ⓧ	105	<u>Struts: campo de formulário sem validador</u>
HasMembro	ⓧ	106	<u>Struts: Plug-in Framework não está em uso</u>
HasMembro	ⓧ	107	<u>Struts: Formulário de validação não utilizado</u>
HasMembro	ⓧ	108	<u>Struts: formulário de ação não validado</u>
HasMembro	ⓧ	109	<u>Struts: validador desativado</u>
HasMembro	ⓧ	110	<u>Struts: Validator sem campo de formulário</u>
HasMembro	Ⓑ	111	<u>Uso direto de JNI inseguro</u>
HasMembro	Ⓑ	112	<u>Validação de XML ausente</u>
HasMembro	Ⓑ	113	<u>Neutralização incorreta de seqüências CRLF em cabeçalhos HTTP ('divisão de resposta HTTP')</u>
HasMembro	Ⓑ	114	<u>Controlo do processo</u>
HasMembro	Ⓑ	115	<u>Interpretação errada da entrada</u>
HasMembro	Ⓒ	116	<u>Codificação imprópria ou escape de saída</u>
HasMembro	Ⓑ	117	<u>Neutralização de saída imprópria para logs</u>
HasMembro	Ⓒ	118	<u>Acesso incorreto do recurso indexável ('Erro de intervalo')</u>
HasMembro	Ⓒ	119	<u>Restrição indevida de operações dentro dos limites de um buffer de memória</u>
HasMembro	Ⓑ	120	<u>Cópia de Buffer sem Verificação do Tamanho da Entrada ('Estouro de</u>

			<u>Buffer Clássico')</u>
HasMembro	V	121	<u>Estouro de buffer com base em pilha</u>
HasMembro	V	122	<u>Excesso de buffer com base em heap</u>
HasMembro	B	123	<u>Escreva-que-onde condição</u>
HasMembro	B	124	<u>Underwrite de buffer ('Buffer Underflow')</u>
HasMembro	B	125	<u>Leitura fora dos limites</u>
HasMembro	V	126	<u>Buffer Over-read</u>
HasMembro	V	127	<u>Buffer Under-read</u>
HasMembro	B	128	<u>Erro de contorno</u>
HasMembro	B	129	<u>Validação imprópria do índice de matriz</u>
HasMembro	B	130	<u>Manipulação imprópria da inconsistência de parâmetro de comprimento</u>
HasMembro	B	131	<u>Cálculo incorreto do tamanho do buffer</u>
HasMembro	B	134	<u>Uso de String de Formato Controlado Externamente</u>
HasMembro	B	135	<u>Cálculo incorreto do comprimento de seqüência de caracteres de vários bytes</u>
HasMembro	C	138	<u>Neutralização indevida de elementos especiais</u>
HasMembro	B	140	<u>Neutralização Indevida de Delimitadores</u>
HasMembro	V	141	<u>Neutralização indevida de delimitadores de parâmetro / argumento</u>

HasMembro	●	142	<u>Neutralização Inadequada de Delimitadores de Valor</u>
HasMembro	●	143	<u>Neutralização indevida de Delimitadores de Registro</u>
HasMembro	●	144	<u>Neutralização Inadequada de Delimitadores de Linhas</u>
HasMembro	●	145	<u>Neutralização inadequada de Delimitadores de Seção</u>
HasMembro	●	146	<u>Neutralização imprópria de Delimitadores de Expressão / Comando</u>
HasMembro	●	147	<u>Neutralização inadequada de terminadores de entrada</u>
HasMembro	●	148	<u>Neutralização inadequada de líderes de entrada</u>
HasMembro	●	149	<u>Neutralização Incorreta da Sintaxe de Citação</u>
HasMembro	●	150	<u>Neutralização indevida de seqüências de escape, meta ou controle</u>
HasMembro	●	151	<u>Neutralização Inadequada de Delimitadores de Comentário</u>
HasMembro	●	152	<u>Neutralização inadequada de símbolos de macro</u>
HasMembro	●	153	<u>Neutralização inadequada de caracteres de substituição</u>
HasMembro	●	154	<u>Neutralização indevida de delimitadores de nomes de variáveis</u>
HasMembro	●	155	<u>Neutralização indevida de curingas ou símbolos correspondentes</u>
HasMembro	●	156	<u>Neutralização inadequada do espaço em branco</u>

HasMembro		157	<u>Falha em Sanitizar Delimitadores Emparelhados</u>
HasMembro		158	<u>Neutralização imprópria de bytes nulos ou caracteres NUL</u>
HasMembro		159	<u>Falha na limpeza do elemento especial</u>
HasMembro		160	<u>Neutralização indevida de elementos especiais importantes</u>
HasMembro		161	<u>Neutralização inadequada de vários elementos especiais importantes</u>
HasMembro		162	<u>Neutralização indevida de elementos especiais de arrasto</u>
HasMembro		163	<u>Neutralização incorreta de vários elementos especiais de arrasto</u>
HasMembro		164	<u>Neutralização inadequada de elementos especiais internos</u>
HasMembro		165	<u>Neutralização incorreta de vários elementos especiais internos</u>
HasMembro		166	<u>Manipulação imprópria de elemento especial ausente</u>
HasMembro		167	<u>Manipulação imprópria do elemento especial adicional</u>
HasMembro		168	<u>Manipulação imprópria de elementos especiais inconsistentes</u>
HasMembro		170	<u>Rescisão Nula Inadequada</u>
HasMembro		172	<u>Erro de codificação</u>
HasMembro		173	<u>Manipulação imprópria de codificação alternativa</u>
HasMembro		174	<u>Decodificação Dupla dos Mesmos Dados</u>

HasMembro	V	175	<u>Manipulação imprópria de codificação mista</u>
HasMembro	V	176	<u>Manipulação imprópria de codificação Unicode</u>
HasMembro	V	177	<u>Manipulação imprópria de codificação de URL (codificação hexadecimal)</u>
HasMembro	B	178	<u>Manipulação imprópria da sensibilidade do caso</u>
HasMembro	B	179	<u>Ordem de Comportamento Incorreta: Validação Antecipada</u>
HasMembro	B	180	<u>Ordem de comportamento incorreta: valide antes de canonizar</u>
HasMembro	B	181	<u>Ordem de Comportamento Incorreta: Validar Antes de Filtrar</u>
HasMembro	B	182	<u>Colapso de dados em valor inseguro</u>
HasMembro	B	183	<u>Whitelist permissiva</u>
HasMembro	B	184	<u>Lista negra incompleta</u>
HasMembro	C	185	<u>Expressão Regular Incorreta</u>
HasMembro	B	186	<u>Expressão Regular excessivamente restritiva</u>
HasMembro	V	187	<u>Comparação Parcial de Cadeia</u>
HasMembro	B	188	<u>Confiança no layout de dados / memória</u>
HasMembro	B	190	<u>Excesso de Inteiro ou Envolvente</u>
HasMembro	B	191	<u>Inferior Inteiro (Wrap ou Wraparound)</u>
HasMembro	C	192	<u>Erro de coerção de inteiro</u>
HasMembro	B	193	<u>Erro off-by-one</u>
HasMembro	B	194	<u>Extensão de sinal inesperada</u>

HasMembro	V	195	<u>Assinado para erro de conversão não assinado</u>
HasMembro	V	196	<u>Não assinado para o erro de conversão assinado</u>
HasMembro	B	197	<u>Erro de truncamento numérico</u>
HasMembro	B	198	<u>Uso de pedidos incorretos de bytes</u>
HasMembro	C	200	<u>Exposição de informação</u>
HasMembro	V	201	<u>Exposição de informação através de dados enviados</u>
HasMembro	V	202	<u>Exposição de dados confidenciais por meio de consultas de dados</u>
HasMembro	C	203	<u>Exposição da informação através da discrepância</u>
HasMembro	B	204	<u>Exposição da informação da discrepância da resposta</u>
HasMembro	B	205	<u>Exposição da informação através da discrepância comportamental</u>
HasMembro	V	206	<u>Exposição da informação do estado interno através da inconsistência comportamental</u>
HasMembro	V	207	<u>Exposição da informação através de uma inconsistência comportamental externa</u>
HasMembro	B	208	<u>Exposição da informação através da discrepância de tempo</u>
HasMembro	B	209	<u>Exposição da informação através de uma mensagem de erro</u>
HasMembro	B	210	<u>Exposição da informação através da mensagem de erro autogerada</u>
HasMembro	B	211	<u>Exposição da informação através da mensagem de erro gerada</u>

			<u>externamente</u>
HasMembro	(B)	212	<u>Remoção transfronteiriça imprópria de dados confidenciais</u>
HasMembro	(B)	213	<u>Exposição intencional de informações</u>
HasMembro	(V)	214	<u>Exposição da informação através do ambiente do processo</u>
HasMembro	(V)	215	<u>Exposição de informações através de informações de depuração</u>
HasMembro	(C)	216	<u>Erros de contenção (erros de contêiner)</u>
HasMembro	(V)	219	<u>Dados confidenciais na raiz da Web</u>
HasMembro	(C)	221	<u>Perda de informação ou omissão</u>
HasMembro	(B)	222	<u>Truncamento de informações relevantes para segurança</u>
HasMembro	(B)	223	<u>Omissão de informações relevantes para a segurança</u>
HasMembro	(B)	224	<u>Informações relevantes sobre segurança obscuras por nome alternativo</u>
HasMembro	(B)	226	<u>Informações confidenciais não esclarecidas antes do lançamento</u>
HasMembro	(C)	228	<u>Manipulação imprópria da estrutura sintaticamente inválida</u>
HasMembro	(B)	229	<u>Manipulação imprópria de valores</u>
HasMembro	(V)	230	<u>Manipulação imprópria de valores ausentes</u>
HasMembro	(V)	231	<u>Manipulação imprópria de valores extras</u>
HasMembro	(V)	232	<u>Manipulação imprópria de valores indefinidos</u>

HasMembro		233	<u>Manipulação imprópria de parâmetros</u>
HasMembro		234	<u>Falha ao lidar com o parâmetro ausente</u>
HasMembro		235	<u>Manipulação imprópria de parâmetros extras</u>
HasMembro		236	<u>Manipulação indevida de parâmetros indefinidos</u>
HasMembro		238	<u>Manipulação imprópria de elementos estruturais incompletos</u>
HasMembro		239	<u>Falha ao lidar com elemento incompleto</u>
HasMembro		240	<u>Manipulação imprópria de elementos estruturais inconsistentes</u>
HasMembro		241	<u>Manipulação imprópria do tipo de dados inesperados</u>
HasMembro		242	<u>Uso da Função Inerentemente Perigosa</u>
HasMembro		243	<u>Criação de Chroot Jail Without Changing Working Directory</u>
HasMembro		244	<u>Limpeza indevida de memória heap antes da liberação ('inspeção de heap')</u>
HasMembro		245	<u>Boas Práticas do J2EE: Gerenciamento Direto de Conexões</u>
HasMembro		246	<u>Boas Práticas do J2EE: Uso Direto dos Soquetes</u>
HasMembro		248	<u>Exceção não capturada</u>
HasMembro		250	<u>Execução com Privilégios Desnecessários</u>

HasMembro		252	<u>Valor de Retorno Não Verificado</u>
HasMembro		253	<u>Verificação incorreta do valor de retorno da função</u>
HasMembro		258	<u>Senha vazia no arquivo de configuração</u>
HasMembro		259	<u>Uso de senha codificada</u>
HasMembro		260	<u>Senha no arquivo de configuração</u>
HasMembro		266	<u>Atribuição de Privilégio Incorreta</u>
HasMembro		267	<u>Privilégio Definido com Ações Não Seguras</u>
HasMembro		268	<u>Encadeamento de Privilégios</u>
HasMembro		269	<u>Gerenciamento impróprio de privilégios</u>
HasMembro		270	<u>Erro de comutação de contexto de privilégio</u>
HasMembro		271	<u>Erros de queda / redução de privilégios</u>
HasMembro		272	<u>Violação pelo Menor Privilégio</u>
HasMembro		273	<u>Verificação imprópria para privilégios descartados</u>
HasMembro		274	<u>Manipulação imprópria de privilégios insuficientes</u>
HasMembro		276	<u>Permissões padrão incorretas</u>
HasMembro		277	<u>Permissões herdadas inseguras</u>
HasMembro		279	<u>Permissões atribuídas à execução incorreta</u>
HasMembro		280	<u>Manipulação indevida de permissões ou privilégios insuficientes</u>
HasMembro		281	<u>Preservação indevida de permissões</u>

HasMembro		284	<u>Controle de Acesso Impróprio</u>
HasMembro		285	<u>Autorização Indevida</u>
HasMembro		286	<u>Gerenciamento incorreto de usuários</u>
HasMembro		287	<u>Autenticação Inadequada</u>
HasMembro		289	<u>Bypass de Autenticação por Nome Alternativo</u>
HasMembro		290	<u>Bypass de Autenticação por Spoofing</u>
HasMembro		295	<u>Validação incorreta de certificado</u>
HasMembro		296	<u>Seguimento impróprio da cadeia de confiança de um certificado</u>
HasMembro		297	<u>Validação imprópria de certificado com incompatibilidade de host</u>
HasMembro		298	<u>Validação imprópria da validade do certificado</u>
HasMembro		299	<u>Verificação indevida de revogação de certificado</u>
HasMembro		302	<u>Bypass de Autenticação por Dados Assumidos-Imutáveis</u>
HasMembro		303	<u>Implementação Incorreta do Algoritmo de Autenticação</u>
HasMembro		304	<u>Etapa crítica ausente na autenticação</u>
HasMembro		305	<u>Bypass de Autenticação por Fraqueza Primária</u>
HasMembro		318	<u>Armazenamento em texto não criptografado de informações confidenciais no executável</u>
HasMembro		325	<u>Etapa criptográfica necessária ausente</u>

HasMembro		329	<u>Não usando um Random IV com o modo CBC</u>
HasMembro		330	<u>Uso de valores aleatórios insuficientes</u>
HasMembro		331	<u>Entropia insuficiente</u>
HasMembro		332	<u>Entropia insuficiente no PRNG</u>
HasMembro		333	<u>Manipulação indevida de entropia insuficiente no TRNG</u>
HasMembro		334	<u>Pequeno espaço de valores aleatórios</u>
HasMembro		335	<u>Uso Incorreto de Sementes no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro		336	<u>Mesma Semente no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro		337	<u>Semente Previsível no Gerador de Números Pseudo-Aleatórios (PRNG)</u>
HasMembro		338	<u>Uso do Gerador de Números Pseudo-Randomizados Criptograficamente Fracos (PRNG)</u>
HasMembro		339	<u>Espaço Pequeno de Semente no PRNG</u>
HasMembro		340	<u>Problemas de Previsibilidade</u>
HasMembro		341	<u>Previsível do estado observável</u>
HasMembro		342	<u>Valor Exato Previsível dos Valores Anteriores</u>
HasMembro		343	<u>Intervalo de valores previsíveis dos valores anteriores</u>
HasMembro		344	<u>Uso de valor invariante em contexto dinamicamente variável</u>

HasMembro		345	<u>Verificação insuficiente de autenticidade de dados</u>
HasMembro		346	<u>Erro de validação de origem</u>
HasMembro		347	<u>Verificação imprópria da assinatura criptográfica</u>
HasMembro		348	<u>Uso de menor fonte confiável</u>
HasMembro		349	<u>Aceitação de dados não confiáveis irrelevantes com dados confiáveis</u>
HasMembro		351	<u>Distinção de Tipo Insuficiente</u>
HasMembro		353	<u>Suporte ausente para verificação de integridade</u>
HasMembro		354	<u>Validação imprópria do valor de verificação de integridade</u>
HasMembro		356	<u>A interface do usuário do produto não avisa o usuário de ações não seguras</u>
HasMembro		357	<u>Aviso de IU insuficiente de operações perigosas</u>
HasMembro		358	<u>Verificação de segurança incorretamente implementada para padrão</u>
HasMembro		359	<u>Exposição de Informações Privadas ('Violação de Privacidade')</u>
HasMembro		360	<u>Confiança dos dados do evento do sistema</u>
HasMembro		362	<u>Execução Concorrente usando Recurso Compartilhado com Sincronização Indevida ('Condição de Corrida')</u>
HasMembro		363	<u>Condição de Corrida Habilitando Link Following</u>

HasMembro		364	<u>Condição de corrida de manipulador de sinal</u>
HasMembro		365	<u>Condição de Corrida no Switch</u>
HasMembro		366	<u>Condição de corrida dentro de um segmento</u>
HasMembro		367	<u>Tempo de verificação Tempo de uso (TOCTOU) Race Condition</u>
HasMembro		368	<u>Condição de Corrida de Comutação de Contexto</u>
HasMembro		369	<u>Dívida por zero</u>
HasMembro		370	<u>Verificação ausente da revogação de certificado após a verificação inicial</u>
HasMembro		372	<u>Distinção Incompleta do Estado Interno</u>
HasMembro		374	<u>Passando objetos mutáveis para um método não confiável</u>
HasMembro		375	<u>Retornando um objeto mutável a um chamador não confiável</u>
HasMembro		377	<u>Arquivo temporário inseguro</u>
HasMembro		378	<u>Criação de arquivo temporário com permissões inseguras</u>
HasMembro		379	<u>Criação de arquivo temporário no diretório com permissões incorretas</u>
HasMembro		382	<u>Boas Práticas do J2EE: Uso de System.exit ()</u>
HasMembro		383	<u>Boas práticas do J2EE: uso direto de threads</u>
HasMembro		384	<u>Fixação de sessão</u>
HasMembro		385	<u>Canal de temporização secreto</u>

HasMembro		386	<u>Nome simbólico não mapeando para corrigir o objeto</u>
HasMembro		390	<u>Detecção da condição de erro sem ação</u>
HasMembro		391	<u>Condição de erro não verificado</u>
HasMembro		392	<u>Relatório de falta de condição de erro</u>
HasMembro		393	<u>Retorno do Código de Status Errado</u>
HasMembro		394	<u>Código de status inesperado ou valor de retorno</u>
HasMembro		395	<u>Uso do NullPointerException Catch para detectar desreferenciamento de ponteiro NULL</u>
HasMembro		396	<u>Declaração de captura para exceção genérica</u>
HasMembro		397	<u>Declaração de lançamentos para exceção genérica</u>
HasMembro		400	<u>Consumo Descontrolado de Recursos ('Exaustão de Recursos')</u>
HasMembro		401	<u>Liberação incorreta de memória antes de remover a última referência ('Memory Leak')</u>
HasMembro		402	<u>Transmissão de recursos privados em uma nova esfera ('vazamento de recursos')</u>
HasMembro		403	<u>Exposição do descritor de arquivo à esfera de controle não intencional ('vazamento de descritor de arquivo')</u>
HasMembro		404	<u>Encerramento ou Liberação Indevida de Recursos</u>

HasMembro		405	<u>Consumo de Recursos Assimétricos (Amplificação)</u>
HasMembro		406	<u>Controle insuficiente de volume de mensagens de rede (amplificação de rede)</u>
HasMembro		407	<u>Complexidade algorítmica</u>
HasMembro		408	<u>Ordem de Comportamento Incorreta: Amplificação Antecipada</u>
HasMembro		409	<u>Manipulação imprópria de dados altamente compactados (amplificação de dados)</u>
HasMembro		410	<u>Pool de recursos insuficiente</u>
HasMembro		412	<u>Bloqueio Acessível Externamente Irrestrito</u>
HasMembro		413	<u>Bloqueio impróprio de recursos</u>
HasMembro		414	<u>Verificação de bloqueio ausente</u>
HasMembro		415	<u>Double Free</u>
HasMembro		416	<u>Use After Free</u>
HasMembro		419	<u>Canal principal desprotegido</u>
HasMembro		420	<u>Canal alternativo desprotegido</u>
HasMembro		425	<u>Solicitação Direta ('Navegação Forçada')</u>
HasMembro		426	<u>Caminho de pesquisa não confiável</u>
HasMembro		427	<u>Elemento do caminho de pesquisa descontrolada</u>
HasMembro		428	<u>Caminho ou elemento de pesquisa sem aspas</u>
HasMembro		430	<u>Implantação do manipulador errado</u>
HasMembro		431	<u>Manipulador ausente</u>

HasMembro		432	<u>Manipulador de sinal perigoso não desativado durante operações confidenciais</u>
HasMembro		433	<u>Entrega de Conteúdo Web Não Unseaded</u>
HasMembro		434	<u>Upload irrestrito de arquivo com tipo perigoso</u>
HasMembro		435	<u>Interação imprópria entre várias entidades que se comportam corretamente</u>
HasMembro		436	<u>Interpretação Conflito</u>
HasMembro		437	<u>Modelo Incompleto de Recursos de Ponto Final</u>
HasMembro		439	<u>Mudança Comportamental em Nova Versão ou Ambiente</u>
HasMembro		440	<u>Violação esperada de comportamento</u>
HasMembro		444	<u>Interpretação Inconsistente de Pedidos HTTP ('HTTP Request Smuggling')</u>
HasMembro		446	<u>Discrepância da interface do usuário para o recurso de segurança</u>
HasMembro		447	<u>Recurso não implementado ou não suportado na interface do usuário</u>
HasMembro		448	<u>Recurso Obsoleto na IU</u>
HasMembro		449	<u>A interface do usuário executa a ação errada</u>
HasMembro		450	<u>Múltiplas Interpretações da Entrada da Interface do Usuário</u>
HasMembro		451	<u>Interface do usuário (IU) Deturpação de informações críticas</u>

HasMembro		453	<u>Inicialização de Variável Padrão Insegura</u>
HasMembro		454	<u>Inicialização Externa de Variáveis Confiáveis ou Armazenamentos de Dados</u>
HasMembro		455	<u>Não-saída na inicialização com falha</u>
HasMembro		456	<u>Inicialização ausente de uma variável</u>
HasMembro		457	<u>Uso de Variável Não Inicializada</u>
HasMembro		459	<u>Limpeza Incompleta</u>
HasMembro		460	<u>Limpeza imprópria na exceção lançada</u>
HasMembro		462	<u>Chave Duplicada na Lista Associativa (Alist)</u>
HasMembro		463	<u>Exclusão da estrutura de dados Sentinel</u>
HasMembro		464	<u>Adição de estrutura de dados Sentinel</u>
HasMembro		466	<u>Retorno do valor do ponteiro fora do intervalo esperado</u>
HasMembro		467	<u>Uso de sizeof () em um tipo de ponteiro</u>
HasMembro		468	<u>Escala de Ponteiros Incorreta</u>
HasMembro		469	<u>Uso de subtração de ponteiro para determinar o tamanho</u>
HasMembro		470	<u>Uso de entrada controlada externamente para selecionar classes ou código ('Reflexão insegura')</u>
HasMembro		471	<u>Modificação de Dados Assumidos-</u>

			<u>Imutáveis (MAID)</u>
HasMembro	Ⓑ	472	<u>Controle Externo do Parâmetro Web Assumido-Imutável</u>
HasMembro	ⓧ	473	<u>Modificação de Variáveis Externas do PHP</u>
HasMembro	Ⓑ	474	<u>Uso de função com implementações inconsistentes</u>
HasMembro	Ⓑ	475	<u>Comportamento indefinido para entrada na API</u>
HasMembro	Ⓑ	476	<u>Desreferência do ponteiro NULL</u>
HasMembro	Ⓑ	477	<u>Uso de Função Obsoleta</u>
HasMembro	ⓧ	478	<u>Caso padrão ausente na instrução de troca</u>
HasMembro	ⓧ	479	<u>Uso de manipulador de sinal de uma função não reentrante</u>
HasMembro	Ⓑ	480	<u>Uso de operador incorreto</u>
HasMembro	ⓧ	481	<u>Atribuição em vez de comparar</u>
HasMembro	ⓧ	482	<u>Comparando em vez de Atribuindo</u>
HasMembro	ⓧ	483	<u>Delimitação de Bloco Incorreta</u>
HasMembro	Ⓑ	484	<u>Declaração de quebra omitida no switch</u>
HasMembro	ⓧ	486	<u>Comparação de Classes por Nome</u>
HasMembro	ⓧ	487	<u>Confiança no escopo no nível do pacote</u>
HasMembro	ⓧ	488	<u>Exposição do Elemento de Dados à Sessão Errada</u>
HasMembro	Ⓑ	489	<u>Código de Depuração de Sobras</u>
HasMembro	ⓧ	491	<u>Método público cloneable () sem final ('Object Hijack')</u>

HasMembro	V	492	<u>Uso da Classe Interna Contendo Dados Sensíveis</u>
HasMembro	V	493	<u>Variável pública crítica sem modificador final</u>
HasMembro	B	494	<u>Download do código sem verificação de integridade</u>
HasMembro	V	495	<u>Campo privado, digitado em matriz, retornado de um método público</u>
HasMembro	V	496	<u>Dados públicos atribuídos ao campo privado digitado por matriz</u>
HasMembro	V	497	<u>Exposição de dados do sistema a uma esfera de controle não autorizada</u>
HasMembro	V	498	<u>Classe Clonável Contendo Informações Sensíveis</u>
HasMembro	V	499	<u>Classe Serializável Contendo Dados Sensíveis</u>
HasMembro	V	500	<u>Campo estático público não marcado final</u>
HasMembro	V	502	<u>Deserialização de dados não confiáveis</u>
HasMembro	C	506	<u>Código Malicioso Integrado</u>
HasMembro	B	507	<u>Cavalo de Tróia</u>
HasMembro	B	508	<u>Código mal-intencionado sem replicação</u>
HasMembro	B	509	<u>Replicando códigos maliciosos (vírus ou worm)</u>
HasMembro	B	510	<u>Alçapão</u>
HasMembro	B	511	<u>Lógica / Time Bomb</u>
HasMembro	B	512	<u>Spyware</u>

HasMembro		514	<u>Canal secreto</u>
HasMembro		515	<u>Canal de Armazenamento Secreto</u>
HasMembro		520	<u>Configuração incorreta do .NET: uso de falsificação de identidade</u>
HasMembro		521	<u>Requisitos de senha fraca</u>
HasMembro		522	<u>Credenciais insuficientemente protegidas</u>
HasMembro		524	<u>Exposição da informação através do cache</u>
HasMembro		525	<u>Exposição de informações através do cache do navegador</u>
HasMembro		526	<u>Exposição da informação através de variáveis ambientais</u>
HasMembro		532	<u>Exposição de informações através de arquivos de log</u>
HasMembro		535	<u>Exposição da informação através da mensagem de erro do escudo</u>
HasMembro		536	<u>Exposição da informação através da mensagem de erro do runtime de Servlet</u>
HasMembro		537	<u>Exposição de informações através da mensagem de erro do Java Runtime</u>
HasMembro		538	<u>Exposição de informações de arquivo e diretório</u>
HasMembro		539	<u>Exposição da informação através de cookies persistentes</u>
HasMembro		540	<u>Exposição da informação através do código fonte</u>
HasMembro		541	<u>Exposição da informação através do código fonte incluído</u>

HasMembro	V	543	<u>Uso do Padrão Singleton Sem Sincronização em um Contexto Multithread</u>
HasMembro	V	546	<u>Comentário Suspeito</u>
HasMembro	V	547	<u>Uso de constantes codificadas e relevantes para segurança</u>
HasMembro	V	548	<u>Exposição de informações por meio da listagem de diretório</u>
HasMembro	V	549	<u>Máscara de campo de senha ausente</u>
HasMembro	V	550	<u>Exposição da informação através da mensagem de erro do servidor</u>
HasMembro	B	551	<u>Ordem de Comportamento Incorreta: Autorização Antes da Análise e Canonização</u>
HasMembro	B	552	<u>Arquivos ou Diretórios Acessíveis a Partes Externas</u>
HasMembro	V	553	<u>Shell de Comando no Diretório Acessível Externamente</u>
HasMembro	V	554	<u>Configuração incorreta do ASP.NET: não usando o Input Validation Framework</u>
HasMembro	V	555	<u>Configuração incorreta de J2EE: Senha de texto sem formatação no arquivo de configuração</u>
HasMembro	V	556	<u>Configuração incorreta do ASP.NET: uso de representação de identidade</u>
HasMembro	V	558	<u>Uso de getlogin () no aplicativo multithread</u>
HasMembro	V	560	<u>Uso de umask () com o argumento chmod-style</u>
HasMembro	V	561	<u>Código Morto</u>

HasMembro		562	<u>Retorno do endereço da variável de pilha</u>
HasMembro		563	<u>Atribuição a variável sem uso</u>
HasMembro		564	<u>Injeção de SQL: Hibernate</u>
HasMembro		565	<u>Confiança em Cookies sem Validação e Verificação de Integridade</u>
HasMembro		566	<u>Bypass de Autorização Através da Chave Primária SQL Controlada pelo Usuário</u>
HasMembro		567	<u>Acesso não sincronizado a dados compartilhados em um contexto multithread</u>
HasMembro		568	<u>finalize () Método sem super.finalize ()</u>
HasMembro		570	<u>Expressão é sempre falsa</u>
HasMembro		571	<u>Expressão é sempre verdadeira</u>
HasMembro		572	<u>Chamar para Thread run () em vez de start ()</u>
HasMembro		573	<u>Seguimento indevido de especificação por chamador</u>
HasMembro		574	<u>Práticas ruins do EJB: uso de primitivas de sincronização</u>
HasMembro		575	<u>Boas Práticas do EJB: Uso do AWT Swing</u>
HasMembro		576	<u>Boas Práticas do EJB: Uso de Java I / O</u>
HasMembro		577	<u>Boas Práticas do EJB: Uso de Soquetes</u>
HasMembro		578	<u>Práticas incorretas do EJB: uso do carregador de classes</u>

HasMembro	V	579	<u>Práticas ruins do J2EE: objeto não serializável armazenado na sessão</u>
HasMembro	V	580	<u>clone () Método sem super.clone ()</u>
HasMembro	B	581	<u>Violação de modelo de objeto: apenas um dos iguais e Hashcode definido</u>
HasMembro	V	582	<u>Matriz Declarada Pública, Final e Estática</u>
HasMembro	V	583	<u>finalize () Método Declarado Público</u>
HasMembro	B	584	<u>Retornar no interior finalmente bloco</u>
HasMembro	V	585	<u>Bloco Sincronizado Vazio</u>
HasMembro	V	586	<u>Chamada explícita para finalizar ()</u>
HasMembro	B	587	<u>Atribuição de um endereço fixo a um ponteiro</u>
HasMembro	V	588	<u>Tentativa de acessar filho de um ponteiro de estrutura não</u>
HasMembro	V	589	<u>Chamada para API não onipresente</u>
HasMembro	V	590	<u>Livre de memória não no heap</u>
HasMembro	V	591	<u>Armazenamento de dados confidenciais em memória bloqueada incorretamente</u>
HasMembro	V	593	<u>Bypass de Autenticação: Objeto OpenSSL CTX Modificado Após a Criação dos Objetos SSL</u>
HasMembro	V	594	<u>J2EE Framework: Salvando Objetos Não Serializáveis no Disco</u>
HasMembro	V	595	<u>Comparação de referências de objetos em vez de conteúdo de objetos</u>
HasMembro	V	597	<u>Uso do Operador Errado na</u>

			<u>Comparação de Cadeias</u>
HasMembro	● V	598	<u>Exposição de informações através de seqüências de caracteres de consulta no pedido GET</u>
HasMembro	● V	599	<u>Validação perdida do certificado OpenSSL</u>
HasMembro	● B	600	<u>Exceção não identificada no Servlet</u>
HasMembro	● V	601	<u>Redirecionamento de URL para site não confiável ('Redirecionamento aberto')</u>
HasMembro	● B	603	<u>Uso da Autenticação do Lado do Cliente</u>
HasMembro	● B	605	<u>Múltiplas Vinculações à Mesma Porta</u>
HasMembro	● B	606	<u>Entrada não verificada para condição de loop</u>
HasMembro	● V	607	<u>Referências do campo final estático público objeto mutável</u>
HasMembro	● V	608	<u>Struts: campo não privado na classe ActionForm</u>
HasMembro	● B	609	<u>Bloqueio com Seleção Dupla</u>
HasMembro	● V	611	<u>Restrição Indevida da Referência de Entidade Externa XML ('XXE')</u>
HasMembro	● V	612	<u>Exposição de informação através da indexação de dados privados</u>
HasMembro	● B	613	<u>Expiração de sessão insuficiente</u>
HasMembro	● V	614	<u>Cookie Sensível em Sessão HTTPS sem Atributo 'Seguro'</u>
HasMembro	● V	615	<u>Exposição da informação através dos comentários</u>
HasMembro	● V	616	<u>Identificação Incompleta de</u>

			<u>Variáveis de Arquivo Carregadas (PHP)</u>
HasMembro	● V	617	<u>Afirmação Alcançável</u>
HasMembro	● B	618	<u>Método ActiveX não seguro exposto</u>
HasMembro	● B	619	<u>Cursor de banco de dados oscilante ('Injeção de cursor')</u>
HasMembro	● V	620	<u>Alteração de senha não confirmada</u>
HasMembro	● B	621	<u>Erro de Extração Variável</u>
HasMembro	● V	622	<u>Validação incorreta de argumentos do gancho de função</u>
HasMembro	● V	623	<u>Controle inseguro do ActiveX marcado como seguro para script</u>
HasMembro	● B	624	<u>Erro de expressão regular executável</u>
HasMembro	● B	625	<u>Expressão Regular Permissiva</u>
HasMembro	● V	626	<u>Erro de Interação de Byte Nulo (Poison Null Byte)</u>
HasMembro	● B	627	<u>Avaliação de Variáveis Dinâmicas</u>
HasMembro	● B	628	<u>Chamada de Função com Argumentos Especificados Incorretamente</u>
HasMembro	● C	636	<u>Não falhando com segurança ('Failing Open')</u>
HasMembro	● C	637	<u>Complexidade Desnecessária no Mecanismo de Proteção (Não Usando 'Economia do Mecanismo')</u>
HasMembro	● C	638	<u>Não usando mediação completa</u>
HasMembro	● B	640	<u>Mecanismo de recuperação de senha fraca para senha esquecida</u>
HasMembro	● B	641	<u>Restrição Incorreta de Nomes para</u>

			<u>Arquivos e Outros Recursos</u>
HasMembro	(C)	642	<u>Controle Externo de Dados Críticos do Estado</u>
HasMembro	(B)	643	<u>Neutralização Indevida de Dados em Expressões XPath ('XPath Injection')</u>
HasMembro	(V)	644	<u>Neutralização incorreta de cabeçalhos HTTP para sintaxe de script</u>
HasMembro	(V)	646	<u>Confiança no nome do arquivo ou na extensão do arquivo fornecido externamente</u>
HasMembro	(V)	647	<u>Uso de Caminhos de URL Não-Canônicos para Decisões de Autorização</u>
HasMembro	(B)	648	<u>Uso incorreto de APIs privilegiadas</u>
HasMembro	(B)	649	<u>Confiança na Ofuscação ou Criptografia de Entradas Relevantes para Segurança sem Verificação de Integridade</u>
HasMembro	(V)	650	<u>Confiando nos métodos de permissão HTTP no lado do servidor</u>
HasMembro	(V)	651	<u>Exposição da informação através do arquivo WSDL</u>
HasMembro	(B)	652	<u>Neutralização Indevida de Dados em Expressões XQuery ('XQuery Injection')</u>
HasMembro	(B)	653	<u>Compartimentalização insuficiente</u>
HasMembro	(B)	654	<u>Dependência de um fator único em uma decisão de segurança</u>
HasMembro	(B)	655	<u>Aceitabilidade Psicológica Insuficiente</u>

HasMembro		656	<u>Confiança na segurança através da obscuridade</u>
HasMembro		657	<u>Violação de Princípios de Design Seguro</u>
HasMembro		662	<u>Sincronização incorreta</u>
HasMembro		663	<u>Uso de uma função não reentrante em um contexto concorrente</u>
HasMembro		664	<u>Controle inadequado de um recurso por toda a sua vida</u>
HasMembro		665	<u>Inicialização incorreta</u>
HasMembro		666	<u>Operação no recurso na fase errada da vida</u>
HasMembro		667	<u>Bloqueio Indevido</u>
HasMembro		668	<u>Exposição de Recurso à Esfera Errada</u>
HasMembro		669	<u>Transferência de recursos incorreta entre esferas</u>
HasMembro		670	<u>Implementação de Fluxo de Controle Sempre Incorreto</u>
HasMembro		671	<u>Falta de controle de administrador sobre segurança</u>
HasMembro		672	<u>Operação em um recurso após a expiração ou liberação</u>
HasMembro		673	<u>Influência Externa da Definição da Esfera</u>
HasMembro		674	<u>Recursão Descontrolada</u>
HasMembro		675	<u>Operações duplicadas no recurso</u>
HasMembro		676	<u>Uso de Função Potencialmente Perigosa</u>

HasMembro		681	<u>Conversão incorreta entre tipos numéricos</u>
HasMembro		682	<u>Cálculo incorreto</u>
HasMembro		683	<u>Chamada de função com ordem incorreta de argumentos</u>
HasMembro		684	<u>Provisão Incorreta de Funcionalidade Especificada</u>
HasMembro		685	<u>Chamada de função com número incorreto de argumentos</u>
HasMembro		686	<u>Chamada de função com tipo de argumento incorreto</u>
HasMembro		687	<u>Chamada de função com valor de argumento especificado incorretamente</u>
HasMembro		688	<u>Chamada de função com variável incorreta ou referência como argumento</u>
HasMembro		689	<u>Condição de corrida de permissão durante a cópia de recurso</u>
HasMembro		690	<u>Valor de Retorno Não Verificado para Retenção de Ponteiro NULL</u>
HasMembro		691	<u>Gerenciamento insuficiente de fluxo de controle</u>
HasMembro		693	<u>Falha do Mecanismo de Proteção</u>
HasMembro		694	<u>Uso de vários recursos com identificador duplicado</u>
HasMembro		695	<u>Uso da funcionalidade de baixo nível</u>
HasMembro		696	<u>Ordem de Comportamento Incorreta</u>
HasMembro		697	<u>Comparação Incorreta</u>
HasMembro		698	<u>Execução após o redirecionamento</u>

			<u>(EAR)</u>
HasMembro		703	<u>Verificação ou manuseio inadequado de condições excepcionais</u>
HasMembro		704	<u>Conversão ou elenco de tipo incorreto</u>
HasMembro		705	<u>Escopo do controle de controle incorreto</u>
HasMembro		706	<u>Uso de Nome ou Referência Resolvidos Incorretamente</u>
HasMembro		707	<u>Aplicação indevida de mensagem ou estrutura de dados</u>
HasMembro		708	<u>Atribuição de propriedade incorreta</u>
HasMembro		710	<u>Aderência inadequada aos padrões de codificação</u>
HasMembro		732	<u>Atribuição de Permissão Incorreta para Recurso Crítico</u>
HasMembro		749	<u>Método perigoso ou função exposta</u>
HasMembro		754	<u>Verificação indevida de condições incomuns ou excepcionais</u>
HasMembro		755	<u>Manipulação indevida de condições excepcionais</u>
HasMembro		759	<u>Uso de um hash unidirecional sem sal</u>
HasMembro		760	<u>Uso de um hash unidirecional com um sal previsível</u>
HasMembro		761	<u>Livre de ponteiro não no início do buffer</u>
HasMembro		762	<u>Rotinas de Gerenciamento de Memória Incompatíveis</u>
HasMembro		763	<u>Liberação de ponteiro ou referência</u>

			<u>inválida</u>
HasMembro	ⓧ	764	<u>Vários bloqueios de um recurso crítico</u>
HasMembro	ⓧ	765	<u>Múltiplos Desbloqueios de um Recurso Crítico</u>
HasMembro	ⓧ	766	<u>Variável Crítica Declarada Pública</u>
HasMembro	ⓧ	767	<u>Acesso à variável privada crítica via método público</u>
HasMembro	ⓧ	768	<u>Avaliação incorreta de curto-circuito</u>
HasMembro	❷	769	<u>Consumo do Descritor de Arquivo Não Controlado</u>
HasMembro	❷	770	<u>Alocação de Recursos sem Limites ou Limitação</u>
HasMembro	❷	771	<u>Referência ausente ao recurso alocado ativo</u>
HasMembro	❷	772	<u>Liberação ausente de recurso após a vida útil efetiva</u>
HasMembro	ⓧ	773	<u>Referência ausente ao descritor de arquivo ativo ou identificador</u>
HasMembro	ⓧ	774	<u>Alocação de descritores de arquivo ou identificadores sem limites ou limitação</u>
HasMembro	ⓧ	775	<u>Liberação ausente do descritor de arquivo ou do identificador após uma vida útil efetiva</u>
HasMembro	ⓧ	776	<u>Restrição Indevida de Referências de Entidade Recursiva em DTDs ('Expansão de Entidade XML')</u>
HasMembro	ⓧ	777	<u>Expressão Regular sem Âncoras</u>
HasMembro	ⓧ	780	<u>Uso do Algoritmo RSA sem OAEP</u>

HasMembro	●	781	<u>Validação incorreta de endereço no IOCTL com código de controle de E / S de METHOD_NEITHER</u>
HasMembro	●	782	<u>IOCTL exposto com controle de acesso insuficiente</u>
HasMembro	●	783	<u>Erro de lógica de precedência do operador</u>
HasMembro	●	784	<u>Confiança em cookies sem validação e verificação de integridade em uma decisão de segurança</u>
HasMembro	●	785	<u>Uso da Função de Manipulação de Caminho sem o Buffer de Tamanho Máximo</u>
HasMembro	●	789	<u>Alocação de Memória Descontrolada</u>
HasMembro	●	790	<u>Filtragem Incorreta de Elementos Especiais</u>
HasMembro	●	791	<u>Filtragem Incompleta de Elementos Especiais</u>
HasMembro	●	792	<u>Filtragem Incompleta de uma ou mais instâncias de elementos especiais</u>
HasMembro	●	793	<u>Filtrando apenas uma instância de um elemento especial</u>
HasMembro	●	794	<u>Filtragem Incompleta de Múltiplas Instâncias de Elementos Especiais</u>
HasMembro	●	795	<u>Filtrando somente elementos especiais em um local especificado</u>
HasMembro	●	796	<u>Filtrando somente elementos especiais em relação a um marcador</u>
HasMembro	●	797	<u>Filtrando apenas elementos especiais em uma posição absoluta</u>

HasMembro		799	<u>Controle inadequado de frequência de interação</u>
HasMembro		804	<u>CAPTCHA adivinhado</u>
HasMembro		805	<u>Acesso de Buffer com Valor de Comprimento Incorreto</u>
HasMembro		806	<u>Acesso ao buffer usando o tamanho do buffer de origem</u>
HasMembro		807	<u>Confiança em entradas não confiáveis em uma decisão de segurança</u>
HasMembro		827	<u>Controle indevido da definição do tipo de documento</u>
HasMembro		829	<u>Inclusão de funcionalidade da esfera de controle não confiável</u>
HasMembro		830	<u>Inclusão de funcionalidade da Web de uma fonte não confiável</u>
HasMembro		836	<u>Uso de hash de senha em vez de senha para autenticação</u>
HasMembro		841	<u>Aplicação indevida do fluxo de trabalho comportamental</u>
HasMembro		842	<u>Posicionamento do usuário em grupo incorreto</u>
HasMembro		843	<u>Acesso do recurso usando o tipo incompatível ('Type Confusion')</u>
HasMembro		862	<u>Autorização ausente</u>
HasMembro		863	<u>Autorização incorreta</u>
HasMembro		908	<u>Uso de recurso não inicializado</u>
HasMembro		909	<u>Inicialização ausente do recurso</u>
HasMembro		910	<u>Uso do Descritor de Arquivo Expirado</u>

HasMembro		911	<u>Atualização incorreta da contagem de referência</u>
HasMembro		912	<u>Funcionalidade oculta</u>
HasMembro		913	<u>Controle impróprio de recursos de código gerenciados dinamicamente</u>
HasMembro		914	<u>Controle impróprio de variáveis dinamicamente identificadas</u>
HasMembro		915	<u>Modificação incorretamente controlada de atributos de objetos determinados dinamicamente</u>
HasMembro		917	<u>Neutralização indevida de elementos especiais usados em uma declaração de linguagem de expressão ('Expression Language Injection')</u>
HasMembro		918	<u>Falsificação de Solicitação do Lado do Servidor (SSRF)</u>
HasMembro		922	<u>Armazenamento Inseguro de Informações Confidenciais</u>
HasMembro		939	<u>Autorização incorreta no manipulador para esquema de URL personalizado</u>
HasMembro		940	<u>Verificação imprópria da fonte de um canal de comunicação</u>
HasMembro		941	<u>Destino especificado incorretamente em um canal de comunicação</u>
HasMembro		942	<u>Whitelist de domínio cruzado excessivamente permissivo</u>
HasMembro		943	<u>Neutralização indevida de elementos especiais na lógica de consulta de dados</u>
HasMembro		1004	<u>Cookie sensível sem sinalizador 'HttpOnly'</u>

HasMembro		1007	<u>Distorção Visual Insuficiente de Homoglifos Apresentados ao Usuário</u>
HasMembro		1021	<u>Restrição Incorreta de Camadas ou Quadros de UI Renderizados</u>
HasMembro		1022	<u>Uso do link da Web para o destino não confiável com o acesso window.opener</u>
HasMembro		1023	<u>Comparação Incompleta com Fatores Perdidos</u>
HasMembro		1024	<u>Comparação de Tipos Incompatíveis</u>
HasMembro		1025	<u>Comparação Usando Fatores Errados</u>

As Vulnerabilidades CWE SANS TOP25 Moat Dangerous Softwares Errors (2011) são:

Classificação	Ponto	Identidade	Nome
[1]	93,8	CWE-89	Neutralização indevida de elementos especiais usados em um comando SQL ('SQL Injection')
[2]	83,3	CWE-78	Neutralização indevida de elementos especiais usados em um comando do sistema operacional ('injeção de comando do sistema operacional')
[3]	79,0	CWE-120	Cópia de Buffer sem Verificação do Tamanho da Entrada ('Estouro de Buffer Clássico')
[4]	77,7	CWE-79	Neutralização incorreta de entrada durante a geração de páginas da Web ('Cross-site Scripting')
[5]	76,9	CWE-306	Autenticação ausente para função crítica
[6]	76,8	CWE-862	Autorização ausente
[7]	75,0	CWE-798	Uso de credenciais codificadas

Classificação	Ponto	Identidade	Nome
[8]	75,0	CWE-311	Ausência de criptografia de dados confidenciais
[9]	74,0	CWE-434	Upload irrestrito de arquivo com tipo perigoso
[10]	73,8	CWE-807	Confiança em entradas não confiáveis em uma decisão de segurança
[11]	73,1	CWE-250	Execução com Privilégios Desnecessários
[12]	70,1	CWE-352	Falsificação de Solicitação Entre Sites (CSRF)
[13]	69,3	CWE-22	Limitação indevida de um nome de caminho para um diretório restrito ('Traversal de caminho')
[14]	68,5	CWE-494	Download do código sem verificação de integridade
[15]	67,8	CWE-863	Autorização incorreta
[16]	66,0	CWE-829	Inclusão de funcionalidade da esfera de controle não confiável
[17]	65,5	CWE-732	Atribuição de Permissão Incorreta para Recurso Crítico
[18]	64,6	CWE-676	Uso de Função Potencialmente Perigosa
[19]	64,1	CWE-327	Uso de Algoritmo Criptográfico Quebrado ou Arriscado
[20]	62,4	CWE-131	Cálculo incorreto do tamanho do buffer
[21]	61,5	CWE-307	Restrição Indevida de Tentativas de Autenticação Excessiva
[22]	61,1	CWE-601	Redirecionamento de URL para site não confiável ('Redirecionamento aberto')
[23]	61,0	CWE-134	String de Formato Descontrolado
[24]	60,3	CWE-190	Excesso de Inteiro ou Envolvente

Classificação	Ponto	Identidade	Nome
[25]	59,9	CWE-759	Uso de um hash unidirecional sem sal

As Vulnerabilidades OWASP Top Ten (2017) são:

1026 - Fraquezas no Top Ten do OWASP (2017)

- + [COWASP Top Ten 2017 Categoria A1 - Injeção - \(1027\)](#)
- + [COWASP Top Ten 2017 Categoria A2 - Autenticação Quebrada - \(1028\)](#)
- + [COWASP Top Ten 2017 Categoria A3 - Exposição Sensível a Dados - \(1029\)](#)
- + [COWASP Top Ten 2017 Categoria A4 - Entidades Externas XML \(XXE\) - \(1030\)](#)
- + [COWASP Top Ten 2017 Categoria A5 - Controle de Acesso Quebrado - \(1031\)](#)
- + [COWASP Top Ten 2017 Categoria A6 - Configuração Incorreta de Segurança - \(1032\)](#)
- + [COWASP Top Ten 2017 Categoria A7 - Cross-Site Scripting \(XSS\) - \(1033\)](#)
- + [COWASP Top Ten 2017 Categoria A8 - Dessorialização Insegura - \(1034\)](#)
 - [COWASP Top Ten 2017 Categoria A9 - Usando Componentes com Vulnerabilidades Conhecidas - \(1035\)](#)
- + [COWASP Top Ten 2017 Categoria A10 - Registro e Monitoramento Insuficiente - \(1036\)](#)

As Vulnerabilidade mais recente da Google Chrome são:

Nome	Descrição
CVE-2017-6753	Uma vulnerabilidade nas extensões de navegador Cisco WebEx para o Google Chrome e o Mozilla Firefox pode permitir que um invasor remoto não autenticado execute código arbitrário com os privilégios do navegador afetado em um sistema afetado. Esta vulnerabilidade afeta as extensões do navegador do Cisco WebEx Meetings Server, dos Cisco WebEx Centers (Centro de Reuniões, Event Center, Training Center e Support Center) e do Cisco WebEx Meetings quando eles estão sendo executados no Microsoft Windows. A vulnerabilidade é devido a um defeito de design na extensão. Um invasor que possa convencer um usuário afetado a visitar uma página da web controlada pelo invasor ou seguir um

Nome	Descrição
	link fornecido pelo invasor com um navegador afetado poderá explorar a vulnerabilidade. Se obtiver êxito, o invasor poderá executar código arbitrário com os privilégios do navegador afetado. As seguintes versões das extensões do navegador Cisco WebEx são afetadas: Versões anteriores à 1.0.12 da extensão Cisco WebEx no Google Chrome, Versões anteriores à 1.0.12 da extensão Cisco WebEx no Mozilla Firefox. IDs de Bug da Cisco: CSCvf15012 CSCvf15020 CSCvf15030 CSCvf15033 CSCvf15036 CSCvf15037.
CVE-2017-5133	A leitura / gravação off-in heap do Blink no Google Chrome anterior ao 62.0.3202.62 permitiu que um invasor remoto corrompesse a memória e, possivelmente, vazasse informações e a possibilidade de executar código por meio de um arquivo PDF criado.
CVE-2017-5132	A implementação inadequada da V8 no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto explorasse potencialmente a corrupção da pilha por meio de uma página HTML criada, também conhecida como manipulação incorreta da pilha do WebAssembly.
CVE-2017-5131	Um estouro de número inteiro no Skia no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada, também conhecida como gravação fora do limite.
CVE-2017-5130	Um estouro de número inteiro em xmlmemory.c na libxml2 anterior à 2.9.5, conforme usado no Google Chrome anterior a 62.0.3202.62 e outros produtos, permitia que um invasor remoto explorasse potencialmente a corrupção da pilha por meio de um arquivo XML criado.
CVE-2017-5129	Um uso depois de liberado no WebAudio no Blink no Google Chrome antes de 62.0.3202.62 permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5128	O estouro do buffer de heap no Blink no Google Chrome anterior ao 62.0.3202.62 permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada para o WebGL.
CVE-2017-5127	O uso posterior do PDFium no Google Chrome antes do 62.0.3202.62 permitia que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo PDF criado.
CVE-2017-5126	Um uso depois de livre no PDFium no Google Chrome antes de 62.0.3202.62 permitia que um invasor remoto explorasse potencialmente a corrupção da pilha por meio de um arquivo PDF criado.
CVE-2017-5125	O estouro de buffer de heap no Skia no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada.

Nome	Descrição
	criada.
CVE-2017-5124	A aplicação incorreta de sandboxing no Blink no Google Chrome antes de 62.0.3202.62 permitiu que um invasor remoto injetasse scripts arbitrários ou HTML (UXSS) por meio de uma página MHTML criada.
CVE-2017-5122	O uso inadequado do tratamento de tamanho de tabela no V8 no Google Chrome anterior ao 61.0.3163.100 para Windows permitiu que um invasor remoto acionasse o acesso fora dos limites por meio de uma página HTML criada.
CVE-2017-5121	O uso inadequado de otimização JIT no V8 no Google Chrome anterior a 61.0.3163.100 para Linux, Windows e Mac permitiu que um invasor remoto executasse código arbitrário dentro de um sandbox por meio de uma página HTML criada, relacionada à fase de análise de escape.
CVE-2017-5120	O uso inadequado de redirecionamentos de incompatibilidade de www na navegação do navegador no Google Chrome anterior a 61.0.3163.79 para Mac, Windows e Linux e 61.0.3163.81 para Android permitiu que um invasor remoto fizesse downgrade de solicitações HTTPS para HTTP por meio de uma página HTML criada. Em outras palavras, o Chrome pode transmitir texto simples mesmo que o usuário tenha inserido um URL https, devido a uma solução mal projetada para casos em que o nome de domínio em um URL quase corresponde ao nome de domínio em um certificado de servidor X.509 (mas difere no inicial "www." substring).
CVE-2017-5119	O uso de um valor não inicializado no Skia no Google Chrome anterior a 61.0.3163.79 para Mac, Windows e Linux e 61.0.3163.81 para Android permitiu que um invasor remoto obtivesse informações potencialmente confidenciais da memória de processo por meio de uma página HTML criada.
CVE-2017-5118	Pisca no Google Chrome antes de 61.0.3163.79 para Mac, Windows e Linux, e 61.0.3163.81 para Android, não propagou corretamente restrições de CSP para páginas de esquema de javascript, o que permitiu que um invasor remoto ignorasse a política de segurança de conteúdo por meio de uma página HTML criada .
CVE-2017-5117	O uso de um valor não inicializado no Skia no Google Chrome anterior a 61.0.3163.79 para Linux e Windows permitiu que um invasor remoto obtivesse informações potencialmente confidenciais da memória de processo por meio de uma página HTML criada.
CVE-2017-5116	O tipo de confusão na V8 no Google Chrome anterior a 61.0.3163.79 para Mac, Windows e Linux e 61.0.3163.81 para Android permitiu que um invasor remoto executasse código arbitrário dentro de uma sandbox por meio de uma página HTML criada.
CVE-2017-5115	O tipo de confusão na V8 no Google Chrome anterior a 61.0.3163.79 para o Windows permitiu que um invasor remoto explorasse potencialmente a corrupção de objetos por meio de

Nome	Descrição
	uma página HTML criada.
CVE-2017-5114	O uso inadequado da alocação de partições no PDFium no Google Chrome anterior a 61.0.3163.79 para Linux, Windows e Mac e 61.0.3163.81 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de memória por meio de um arquivo PDF criado.
CVE-2017-5113	O estouro de matemática no Skia no Google Chrome anterior a 61.0.3163.79 para Mac, Windows e Linux e 61.0.3163.81 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção da pilha por meio de uma página HTML criada.
CVE-2017-5112	O estouro de buffer de heap no WebGL no Google Chrome anterior a 61.0.3163.79 para o Windows permitiu que um invasor remoto executasse código arbitrário dentro de um sandbox por meio de uma página HTML criada.
CVE-2017-5111	Um uso depois do Free no PDFium no Google Chrome anterior a 61.0.3163.79 para Linux, Windows e Mac permitiu que um invasor remoto explorasse potencialmente a corrupção de memória por meio de um arquivo PDF criado.
CVE-2017-5110	A implementação inadequada da API de pagamentos da Web em blob: e dados: esquemas no Web Payments no Google Chrome anteriores a 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um invasor remoto falsificasse o conteúdo da omnibox por meio de uma página HTML criada .
CVE-2017-5109	A implementação inadequada do manuseio do manipulador de descarregamento nos prompts de permissão do Google Chrome anteriores a 60.0.3112.78 para Linux, Windows e Mac permitiu que um invasor remoto exibisse a interface do usuário em uma guia não controlada pelo invasor por meio de uma página HTML criada.
CVE-2017-5108	A confusão do tipo no PDFium no Google Chrome anterior a 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um invasor remoto modificasse de maneira potencialmente maliciosa os objetos por meio de um arquivo PDF criado.
CVE-2017-5107	Um ataque de temporização na renderização de SVG no Google Chrome anterior a 60.0.3112.78 para Linux, Windows e Mac permitiu que um invasor remoto extraísse valores de pixel de uma página de origem cruzada, sendo convertida em iframe por meio de uma página HTML criada.
CVE-2017-5106	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um invasor remoto executasse a falsificação de domínio por meio de homógrafos com IDN em um nome de domínio elaborado.
CVE-2017-5105	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um invasor remoto executasse a falsificação de domínio por meio de homógrafos com IDN em um nome de

Nome	Descrição
	domínio elaborado.
CVE-2017-5104	A implementação inadequada em intersticiais no Google Chrome anterior a 60.0.3112.78 para Mac permitiu que um invasor remoto falsificasse o conteúdo da omnibox por meio de uma página HTML criada.
CVE-2017-5103	O uso de um valor não inicializado no Skia no Google Chrome anterior a 60.0.3112.78 para Linux, Windows e Mac permitiu que um invasor remoto obtivesse informações potencialmente confidenciais da memória de processo por meio de uma página HTML criada.
CVE-2017-5102	O uso de um valor não inicializado no Skia no Google Chrome antes de 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um invasor remoto obtivesse informações potencialmente confidenciais da memória de processo por meio de uma página HTML criada.
CVE-2017-5101	A implementação inadequada na Omnibox no Google Chrome anterior a 60.0.3112.78 para Linux, Windows e Mac permitiu que um invasor remoto falsificasse o conteúdo da Omnibox por meio de uma página HTML criada.
CVE-2017-5100	Um uso depois de gratuito no Google Apps no Google Chrome anterior a 60.0.3112.78 para o Windows permitia que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5099	A validação insuficiente de entradas não fidedignas nos Plug-ins PPAPI no Google Chrome anteriores a 60.0.3112.78 para Mac permitiu que um atacante remoto obtivesse potencialmente a elevação de privilégios através de uma página HTML elaborada.
CVE-2017-5098	Um uso após o V8 gratuito no Google Chrome antes de 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5097	A validação insuficiente de entrada não confiável no Skia no Google Chrome anterior a 60.0.3112.78 para Linux permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5096	A aplicação insuficiente de políticas durante a navegação entre diferentes esquemas no Google Chrome anteriores a 60.0.3112.78 para Android permitiu que um invasor remoto efetuasse o download de conteúdo de origem cruzada por meio de uma página HTML elaborada, relacionada a intenções.
CVE-2017-5095	O estouro de pilha no PDFium no Google Chrome anterior a 60.0.3112.78 para Linux, Windows e Mac permitiu que um invasor remoto explorasse potencialmente a corrupção de pilha por meio de um arquivo PDF criado.
CVE-2017-5094	Tipo de confusão nas extensões As vinculações do JavaScript no Google Chrome anteriores a 60.0.3112.78 para Mac, Windows,

Nome	Descrição
	Linux e Android permitiram que um invasor remoto modificasse, de maneira mal-intencionada, os objetos por meio de uma página HTML criada.
CVE-2017-5093	A implementação inadequada no processamento de diálogos modais no Blink no Google Chrome antes de 60.0.3112.78 para Mac, Windows, Linux e Android permitiu que um atacante remoto impedisse que um aviso de tela cheia fosse exibido por meio de uma página HTML criada.
CVE-2017-5092	A validação insuficiente de entradas não confiáveis nos plug-ins de PPAPI no Google Chrome anteriores a 60.0.3112.78 para o Windows permitiu que um invasor remoto realizasse um escape de sandbox por meio de uma página HTML criada.
CVE-2017-5091	Um uso depois de gratuito no IndexedDB no Google Chrome anterior a 60.0.3112.78 para Linux, Android, Windows e Mac permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5090	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 59.0.3071.115 para Mac permitiu que um invasor remoto executasse a falsificação de domínio por meio de um nome de domínio criado contendo um caractere U + 0620, também conhecido como problema 32458012 da Apple.
CVE-2017-5089	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 59.0.3071.104 para Mac permitiu que um invasor remoto executasse a falsificação de domínio por meio de um nome de domínio elaborado.
CVE-2017-5088	A validação insuficiente de entradas não confiáveis no V8 no Google Chrome anterior a 59.0.3071.104 para Mac, Windows e Linux e 59.0.3071.117 para Android permitiu que um invasor remoto realizasse um acesso à memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5087	Um uso depois de liberado no Blink no Google Chrome antes de 59.0.3071.104 para Mac, Windows e Linux, e 59.0.3071.117 para o Android, permitia que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada por um DLL. escape sandbox.
CVE-2017-5086	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 59.0.3071.86 para Windows e Mac permitiu que um invasor remoto executasse a falsificação de domínio por meio de homógrafos com IDN em um nome de domínio elaborado.
CVE-2017-5085	A implementação inadequada nos marcadores do Google Chrome anteriores a 59 para iOS permitiu que um invasor remoto convencesse o usuário a executar determinadas operações para executar o JavaScript em chrome: // páginas por meio de um marcador elaborado.
CVE-2017-5084	A implementação inadequada no gravador de imagens no Google Chrome OS anterior a 59.0.3071.92 permitiu que um invasor local lesse arquivos locais via comandos dbus-send para um ponto final

Nome	Descrição
	do BurnImage D-Bus.
CVE-2017-5083	A implementação inadequada no Blink no Google Chrome anterior a 59.0.3071.86 para Mac, Windows e Linux, e 59.0.3071.92 para Android, permitiu que um invasor remoto exibisse a interface do usuário em uma guia não controlada pelo invasor por meio de uma página HTML criada.
CVE-2017-5082	O não aproveitamento das atenuações disponíveis no preenchimento automático do cartão de crédito no Google Chrome anteriores a 59.0.3071.92 para Android permitiu que um invasor local capturasse as capturas de tela das informações do cartão de crédito por meio de uma página HTML elaborada.
CVE-2017-5081	A falta de verificação da pasta de localidade de uma extensão no Google Chrome anterior a 59.0.3071.86 para Mac, Windows e Linux e 59.0.3071.92 para Android permitiu que um invasor com acesso de gravação local modificasse as extensões modificando os arquivos de extensão.
CVE-2017-5080	Um uso após o preenchimento automático do cartão de crédito no Google Chrome antes de 59.0.3071.86 para Linux e Windows permitia que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5079	A implementação inadequada no Blink no Google Chrome anterior a 59.0.3071.86 para Mac, Windows e Linux, e 59.0.3071.92 para Android, permitiu que um invasor remoto exibisse a interface do usuário em uma guia não controlada pelo invasor por meio de uma página HTML criada.
CVE-2017-5078	Validação insuficiente de entrada não confiável no mailto de Blink: o tratamento no Google Chrome anterior a 59.0.3071.86 para Linux, Windows e Mac permitiu que um invasor remoto executasse a injeção de comando por meio de uma página HTML criada, um problema semelhante ao CVE-2004-0121. Por exemplo, caracteres como * têm uma interação incorreta com xdg-email no xdg-utils e um caractere de espaço pode ser usado na frente de um argumento de linha de comando.
CVE-2017-5077	A validação insuficiente de entradas não confiáveis no Skia no Google Chrome anteriores a 59.0.3071.86 para Linux, Windows e Mac e 59.0.3071.92 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5076	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 59.0.3071.86 para Mac, Windows e Linux e 59.0.3071.92 para Android permitiu que um invasor remoto executasse falsificação de domínio por meio de homógrafos IDN em um nome de domínio elaborado.
CVE-2017-5075	A implementação inadequada nos relatórios de CSP no Blink no Google Chrome anteriores a 59.0.3071.86 para Linux, Windows e Mac e 59.0.3071.92 para Android permitiu que um invasor remoto obtivesse o valor de fragmentos de URL por meio de uma página

Nome	Descrição
	HTML criada.
CVE-2017-5074	Um uso depois de gratuito nos aplicativos do Google Chrome no Google Chrome anteriores a 59.0.3071.86 para Windows permitia que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada por ele, relacionada ao Bluetooth.
CVE-2017-5073	O uso depois da visualização gratuita no Blink no Google Chrome antes de 59.0.3071.86 para Linux, Windows e Mac e 59.0.3071.92 para Android permitia que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5072	A implementação inadequada na Omnibox no Google Chrome anterior a 59.0.3071.92 para Android permitiu que um invasor remoto executasse a falsificação de domínio com caracteres RTL por meio de uma página de URL criada.
CVE-2017-5071	A validação insuficiente de entradas não confiáveis no V8 no Google Chrome anteriores a 59.0.3071.86 para Linux, Windows e Mac e 59.0.3071.92 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5070	O tipo de confusão na V8 no Google Chrome anterior a 59.0.3071.86 para Linux, Windows e Mac e 59.0.3071.92 para Android permitiu que um invasor remoto executasse código arbitrário dentro de uma sandbox por meio de uma página HTML criada.
CVE-2017-5069	O tipo MIME incorreto de relatórios de Proteção XSS no Blink no Google Chrome anterior a 58.0.3029.81 para Linux, Windows e Mac e 58.0.3029.83 para Android permitiu que um invasor remoto contornasse as verificações de Compartilhamento de Recursos de Origem Cruzada por meio de uma página HTML criada .
CVE-2017-5068	O tratamento incorreto do ID de imagem no WebRTC no Google Chrome antes de 58.0.3029.96 para Mac, Windows e Linux permitiu que um invasor remoto acionasse uma condição de corrida por meio de uma página HTML criada.
CVE-2017-5067	Um cronômetro de watchdog insuficiente na navegação no Google Chrome anterior a 58.0.3029.81 para Linux, Windows e Mac permitiu que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de uma página HTML criada.
CVE-2017-5066	Verificações de consistência insuficientes no processamento de assinaturas na pilha de rede do Google Chrome anteriores a 58.0.3029.81 para Mac, Windows e Linux e 58.0.3029.83 para Android permitiram que um invasor remoto aceitasse incorretamente um certificado X.509 mal formado por meio de um trabalho Página HTML.
CVE-2017-5065	A falta de uma ação apropriada na navegação de página no Blink no Google Chrome antes de 58.0.3029.81 para Windows e Mac permitiu que um invasor remoto confundisse um usuário com uma

Nome	Descrição
CVE-2017-5064	decisão incorreta de segurança por meio de uma página HTML criada.
CVE-2017-5063	O tratamento incorreto das alterações do DOM no Blink no Google Chrome anteriores a 58.0.3029.81 para o Windows permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada.
CVE-2017-5062	Um estouro numérico no Skia no Google Chrome anterior a 58.0.3029.81 para Linux, Windows e Mac e 58.0.3029.83 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5061	Um uso depois de gratuito nos Aplicativos do Google Chrome no Google Chrome anteriores a 58.0.3029.81 para Mac, Windows e Linux e 58.0.3029.83 para Android permitiu que um invasor remoto realizasse um acesso à memória fora dos limites por meio de uma extensão do Chrome criada.
CVE-2017-5060	Uma condição de corrida na navegação no Google Chrome anterior a 58.0.3029.81 para Linux, Windows e Mac permitiu que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de uma página HTML criada.
CVE-2017-5059	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 58.0.3029.81 para Mac, Windows e Linux e 58.0.3029.83 para Android permitiu que um invasor remoto executasse a falsificação de domínio por meio de homógrafos com IDN em um nome de domínio elaborado.
CVE-2017-5058	Tipo de confusão no Blink no Google Chrome antes de 58.0.3029.81 para Linux, Windows e Mac e 58.0.3029.83 para o Android, permitiu que um invasor remoto potencialmente obter execução de código através de uma página HTML trabalhada.
CVE-2017-5057	Um uso depois de liberado no PrintPreview no Google Chrome antes de 58.0.3029.81 para o Windows permitiu que um invasor remoto realizasse potencialmente o acesso à memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5056	Tipo confusão no PDFium no Google Chrome antes de 58.0.3029.81 para Mac, Windows e Linux, e 58.0.3029.83 para o Android, permitiu um atacante remoto para realizar uma leitura de memória fora dos limites através de um arquivo PDF criado.
CVE-2017-5055	Um uso depois de liberado no Blink no Google Chrome anterior a 57.0.2987.133 para Linux, Windows e Mac e 57.0.2987.132 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5054	Um uso depois de liberado no Blink no Google Chrome anterior a 57.0.2987.133 para Linux e Windows permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.

Nome	Descrição
CVE-2017-5053	Android permitiu que um invasor remoto obtivesse conteúdo de memória heap por meio de uma página HTML criada.
CVE-2017-5052	Uma leitura de fora do limite na V8 no Google Chrome anterior a 57.0.2987.133 para Linux, Windows e Mac e 57.0.2987.132 para Android permitiu que um invasor remoto executasse código arbitrário dentro de uma sandbox por meio de uma página HTML criada, relacionada para <code>Array.prototype.indexOf</code> .
CVE-2017-5051	Uma suposição incorreta sobre a estrutura de bloqueio no Blink no Google Chrome anterior a 57.0.2987.133 para Mac, Windows e Linux e 57.0.2987.132 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de memória por meio de uma página HTML criada que acionasse a conversão incorreta.
CVE-2017-5050	Um estouro de inteiro no FFmpeg no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto executasse uma gravação de memória fora do limite por meio de um arquivo de vídeo criado, relacionado ao <code>ChunkDemuxer</code> .
CVE-2017-5049	Um estouro de inteiro no FFmpeg no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto executasse uma gravação de memória fora do limite por meio de um arquivo de vídeo criado, relacionado ao <code>ChunkDemuxer</code> .
CVE-2017-5048	Um estouro de inteiro no FFmpeg no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto executasse uma gravação de memória fora do limite por meio de um arquivo de vídeo criado, relacionado ao <code>ChunkDemuxer</code> .
CVE-2017-5047	Um estouro de inteiro no FFmpeg no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto executasse uma gravação de memória fora do limite por meio de um arquivo de vídeo criado, relacionado ao <code>ChunkDemuxer</code> .
CVE-2017-5046	A V8 no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android teve aplicação de política insuficiente, o que permitiu a um atacante remoto falsificar o objeto de localização por meio de uma página HTML criada, relacionada à divulgação de informações do Blink.
CVE-2017-5045	O XSS Auditor no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu a detecção de um carregamento de iframe bloqueado, que permitiu a um atacante remoto aplicar variáveis JavaScript de força bruta por

Nome	Descrição
	meio de uma página HTML criada.
CVE-2017-5044	O estouro de buffer de heap no processamento de filtro no Skia no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5043	Os aplicativos do Google Chrome no Google Chrome anteriores a 57.0.2987.98 para Linux, Windows e Mac tiveram um uso após o bug gratuito no GuestView, que permitia que um invasor remoto realizasse uma leitura de memória fora do limite por meio de uma extensão do Chrome criada.
CVE-2017-5042	O Google Cast no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android enviou cookies para sites descobertos por SSDP, o que permitiu que um invasor no segmento de rede local iniciasse conexões com URLs arbitrários e observasse qualquer cookie de texto sem formatação envie.
CVE-2017-5041	O Google Chrome anterior a 57.0.2987.100 processou incorretamente a navegação retroativa, o que permitiu que um invasor remoto exibisse informações incorretas para um site por meio de uma página HTML criada.
CVE-2017-5040	O V8 no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para o Android não continha uma verificação de castração, que permitia a um invasor remoto ler valores na memória por meio de uma página HTML criada.
CVE-2017-5039	Um uso depois de gratuito no PDFium no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo PDF criado.
CVE-2017-5038	Os aplicativos do Google Chrome no Google Chrome anteriores a 57.0.2987.98 para Linux, Windows e Mac tiveram um uso após o bug gratuito no GuestView, que permitia que um invasor remoto realizasse uma leitura de memória fora do limite por meio de uma extensão do Chrome criada.
CVE-2017-5037	Um estouro de inteiro no FFmpeg no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto executasse uma gravação de memória fora do limite por meio de um arquivo de vídeo criado, relacionado ao ChunkDemuxer.
CVE-2017-5036	Um uso depois de gratuito no PDFium no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android permitiu que um invasor remoto tivesse um impacto não especificado por meio de um arquivo PDF criado.
CVE-2017-5035	O Google Chrome anterior a 57.0.2987.98 para Windows e Mac tinha uma condição de corrida, o que poderia fazer com que o Chrome exibisse informações de certificado incorretas para um

Nome	Descrição
	site.
CVE-2017-5034	Um uso após o livre no PDFium no Google Chrome anterior a 57.0.2987.98 para Linux e Windows permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de um arquivo PDF criado.
CVE-2017-5033	Pisca no Google Chrome antes de 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android não propagou corretamente restrições de CSP para páginas de esquema local, o que permitiu que um atacante remoto ignorasse a política de segurança de conteúdo por meio de uma página HTML trabalhada para a palavra-chave insegura.
CVE-2017-5032	O PDFium no Google Chrome anterior a 57.0.2987.98 para Windows poderia ser feito para incrementar o fim de um buffer, o que permitia a um invasor remoto explorar potencialmente a corrupção de heap por meio de um arquivo PDF criado.
CVE-2017-5031	Um uso depois de liberado em ANGLE no Google Chrome antes de 57.0.2987.98 para o Windows permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5030	O tratamento incorreto de espécies complexas na V8 no Google Chrome anterior a 57.0.2987.98 para Linux, Windows e Mac e 57.0.2987.108 para Android permitiu que um invasor remoto executasse código arbitrário por meio de uma página HTML criada.
CVE-2017-5029	A função xsltAddTextString em transform.c na libxslt 1.1.29, como usada no Blink no Google Chrome anterior a 57.0.2987.98 para Mac, Windows e Linux e 57.0.2987.108 para Android, não tinha uma verificação de estouro de número inteiro durante um cálculo de tamanho, que permitia que um invasor remoto executasse uma gravação de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5027	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, não conseguiu aplicar corretamente a política de segurança de conteúdo in-line, o que permitiu que um atacante remoto ignorasse a política de segurança de conteúdo através de uma página HTML criada.
CVE-2017-5026	O Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac falhou em impedir que os alertas fossem exibidos por quadros trocados, o que permitia que um invasor remoto mostrasse alertas em uma página que eles não controlam por meio de uma página HTML criada.
CVE-2017-5025	O FFmpeg no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac falhou ao executar a verificação de limites adequada, o que permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo de vídeo criado.
CVE-2017-5024	O FFmpeg no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac falhou ao executar a verificação de limites

Nome	Descrição
	adequada, o que permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo de vídeo criado.
CVE-2017-5023	Digite confusão no Histograma no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, permitiu que um invasor remoto explorasse potencialmente uma desreferência quase nula por meio de uma página HTML criada.
CVE-2017-5022	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, não conseguiu aplicar corretamente a política de segurança de conteúdo in-line, o que permitiu que um atacante remoto ignorasse a política de segurança de conteúdo através de uma página HTML criada.
CVE-2017-5021	Um uso depois de gratuito no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5020	O Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, não exigia um gesto do usuário para poderosas operações de download, o que permitia a um invasor remoto convencer um usuário a instalar uma extensão maliciosa para executar código arbitrário através de uma página HTML criada.
CVE-2017-5019	Um uso depois de gratuito no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada.
CVE-2017-5018	O Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android tinha uma política de segurança de conteúdo insuficientemente rigorosa na página inicializadora de aplicativos do Chrome, que permitia a um invasor remoto inserir scripts ou HTML em uma página privilegiada por meio de uma página HTML criada
CVE-2017-5017	As interações com o sistema operacional no Google Chrome antes de 56.0.2924.76 para o Mac insuficientemente limpam a memória de vídeo, o que permitiu que um invasor remoto extraísse fragmentos de imagem em sistemas com chips gráficos GeForce 8600M por meio de uma página HTML criada.
CVE-2017-5016	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, não conseguiu impedir que certos elementos da interface do usuário fossem exibidos por páginas não visíveis, o que permitiu que um invasor remoto mostrasse certos elementos da interface do usuário em um página que eles não controlam por meio de uma página HTML criada.
CVE-2017-5015	O Google Chrome anterior a 56.0.2924.76 para Linux, Windows e

Nome	Descrição
	Mac e 56.0.2924.87 para Android, manipulava incorretamente os glifos Unicode, o que permitia que um invasor remoto executasse a falsificação de domínio por meio de homógrafos IDN em um nome de domínio elaborado.
CVE-2017-5014	O estouro de buffer de heap durante o processamento de imagem no Skia no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-5013	O Google Chrome anterior a 56.0.2924.76 para o Linux manipulou incorretamente novas navegações de páginas de guias em guias não selecionadas, o que permitiu que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de uma página HTML criada.
CVE-2017-5012	Um estouro de buffer de heap na V8 no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção da pilha por meio de uma página HTML criada.
CVE-2017-5011	O Google Chrome antes de 56.0.2924.76 para o Windows insuficientemente higienizado DevTools URLs, o que permitiu um atacante remoto que convenceu um usuário a instalar uma extensão maliciosa para ler o conteúdo do sistema de arquivos através de uma página HTML trabalhada.
CVE-2017-5010	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, resolveu promessas em um contexto inadequado, que permitia a um invasor remoto injetar scripts arbitrários ou HTML (UXSS) por meio de uma página HTML criada.
CVE-2017-5009	O WebRTC no Google Chrome anterior a 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android não conseguiu executar a verificação de limites adequada, o que permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada.
CVE-2017-5008	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, permitindo que JavaScript controlado pelo invasor seja executado durante a invocação de um método de script privado, que permite que um invasor remoto injete scripts arbitrários ou HTML (UXSS) através de uma página HTML criada.
CVE-2017-5007	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, manipulou incorretamente a sequência de eventos ao fechar uma página, o que permitiu que um invasor remoto injetasse scripts arbitrários ou HTML (UXSS) por meio de um página HTML trabalhada.
CVE-2017-5006	Pisca no Google Chrome antes de 56.0.2924.76 para Linux, Windows e Mac e 56.0.2924.87 para Android, tratou

Nome	Descrição
	incorretamente relacionamentos com proprietários de objetos, o que permitiu que um invasor remoto injetasse scripts arbitrários ou HTML (UXSS) por meio de uma página HTML criada.
CVE-2017-3823	Foi descoberto um problema no Cisco WebEx Extension anterior ao 1.0.7 no Google Chrome, no Contêiner de plug-ins do ActiveTouch General antes do 106 no Mozilla Firefox, no plug-in de controle ActiveX da classe GpcContainer antes do 10031.6.2017.0126 no Internet Explorer e no plug-in de controle ActiveX do gerenciador de download antes 2.1.0.10 no Internet Explorer. Uma vulnerabilidade nessas extensões de navegador Cisco WebEx pode permitir que um invasor remoto não autenticado execute código arbitrário com os privilégios do navegador afetado em um sistema afetado. Essa vulnerabilidade afeta as extensões de navegador do Cisco WebEx Meetings Server e dos Cisco WebEx Centers (Centro de Reuniões, Central de Eventos, Training Center e Centro de Suporte) quando eles estão sendo executados no Microsoft Windows. A vulnerabilidade é um defeito de design em um analisador de resposta de interface de programação de aplicativo (API) dentro da extensão. Um invasor que pode convencer um usuário afetado a visitar uma página da web controlada pelo invasor ou seguir um link fornecido pelo invasor com um navegador afetado pode explorar a vulnerabilidade. Se obtiver êxito, o invasor poderá executar código arbitrário com os privilégios do navegador afetado.
CVE-2017-15400	A restrição insuficiente de filtros IPP no CUPS no Google Chrome OS anterior a 62.0.3202.74 permitiu que um invasor remoto executasse um comando com os mesmos privilégios do daemon cups por meio de um arquivo PPD criado, também conhecido como um problema CRLF da impressora zeroconfig.
CVE-2017-15397	A implementação inadequada do ChromeVox no Google Chrome OS anterior ao 62.0.3202.74 permitiu que um invasor remoto em uma posição de rede privilegiada observasse ou adulterasse determinadas solicitações HTTP de texto não criptografado, aproveitando essa posição.
CVE-2017-15395	Um uso depois de liberado no Blink no Google Chrome antes de 62.0.3202.62 permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada, também conhecida como um cancelamento de referência do ponteiro ImageCapture NULL.
CVE-2017-15394	A Insuficiente Imposição de Política em Extensões no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto executasse falsificação de domínio em caixas de diálogo de permissão por meio de homógrafos de IDN em uma Extensão do Chrome criada.
CVE-2017-15393	A aplicação insuficiente de políticas na depuração remota do Devtools no Google Chrome anterior à 62.0.3202.62 permitiu que um invasor remoto obtivesse acesso à funcionalidade de depuração remota por meio de uma página HTML criada por ele, também

Nome	Descrição
	conhecida como vazamento de Referer.
CVE-2017-15392	A validação insuficiente de dados na V8 no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor que pudesse gravar no Registro do Windows explorasse potencialmente a corrupção da pilha por meio de uma entrada do Registro do Windows criada para o Managed Platform, relacionada à PlatformIntegration.
CVE-2017-15391	A aplicação insuficiente de políticas em extensões no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto acessasse páginas de extensão sem autorização por meio de uma página HTML criada.
CVE-2017-15390	A aplicação insuficiente de políticas na omnibox no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto executasse falsificação de domínio por meio de homógrafos com IDN em um nome de domínio elaborado.
CVE-2017-15389	Um cronômetro de watchdog insuficiente na navegação no Google Chrome anterior a 62.0.3202.62 permitiu que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de uma página HTML criada.
CVE-2017-15388	A iteração por meio de pontos não finitos no Skia no Google Chrome anteriores a 62.0.3202.62 permitia que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2017-15387	A aplicação insuficiente da Política de segurança de conteúdo no Blink no Google Chrome antes de 62.0.3202.62 permitiu que um invasor remoto abrisse o javascript: janelas de URL quando não deveriam ter permissão por meio de uma página HTML criada.
CVE-2017-15386	A implementação incorreta no Blink no Google Chrome anterior ao 62.0.3202.62 permitiu que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de uma página HTML criada.
CVE-2016-9650	Pisca no Google Chrome antes de 55.0.2883.75 para Mac, Windows e Linux, e 55.0.2883.84 para o Android manipulou incorretamente iframes, o que permitiu que um invasor remoto ignorasse uma política de não-referenciador por meio de uma página HTML criada.
CVE-2016-7549	O Google Chrome anterior a 53.0.2785.113 não garante que o destinatário de uma determinada mensagem IPC seja um RenderFrame ou RenderWidget válido, o que permite que atacantes remotos causem uma negação de serviço (desreferimento inválido de ponteiro e falha de aplicativo) ou possivelmente outro impacto não especificado, aproveitando acesso a um processo de renderização, relacionado a render_frame_host_impl.cc e render_widget_host_impl.cc, conforme demonstrado por uma mensagem do Gerenciador de Senhas.
CVE-2016-7395	SkPath.cpp no Skia, como usado no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes 53.0.2785.92 no Linux, não valida corretamente os valores de retorno de chamadas

Nome	Descrição
	ChopMonoAtY, o que permite que atacantes remotos causem uma negação de serviço (acesso de memória não inicializado e falha de aplicativo) ou possivelmente não especificou outro impacto por meio de dados gráficos criados.
CVE-2016-5226	Pisca no Google Chrome antes de 55.0.2883.75 para Linux, Windows e Mac executado javascript: URLs inseridos na barra de URL no contexto da guia atual, que permitia a um usuário de engenharia social fazer o XSS arrastando e soltando um URL javascript: a barra de URL.
CVE-2016-5225	Pisca no Google Chrome antes de 55.0.2883.75 para Mac, Windows e Linux, e 55.0.2883.84 para Android tratou incorretamente ações de formulário, o que permitiu que um invasor remoto ignorasse a Política de segurança de conteúdo por meio de uma página HTML criada.
CVE-2016-5224	Um ataque de temporização na aritmética de ponto flutuante desnormalizado em filtros SVG no Blink no Google Chrome antes de 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um atacante remoto ignorasse a Política de mesma origem por meio de uma página HTML criada.
CVE-2016-5223	O estouro de inteiro no PDFium no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap ou DoS por meio de um arquivo PDF criado.
CVE-2016-5222	O tratamento incorreto de URLs inválidos no Google Chrome anteriores a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de uma página HTML criada.
CVE-2016-5221	O tipo de confusão em libGLESv2 em ANGLE no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android possivelmente permitiu que um invasor remoto ignorasse a validação do buffer por meio de uma página HTML criada.
CVE-2016-5220	O PDFium no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android tratava incorretamente a navegação em PDFs, o que permitia que um invasor remoto lesse arquivos locais por meio de um arquivo PDF criado.
CVE-2016-5219	Um uso de pilha depois de liberado na V8 no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção da pilha por meio de uma página HTML criada.
CVE-2016-5218	A API de extensões no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android tratava incorretamente a navegação em PDFs, o que permitia que um

Nome	Descrição
	invasor remoto falsificasse temporariamente o conteúdo da omnibox (barra de URL) por meio de um trabalho Página HTML contendo dados PDF.
CVE-2016-5217	A API de extensões do Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitia o acesso incorreto a plug-ins privilegiados, o que permitia que um invasor remoto ignorasse o isolamento do site por meio de uma página HTML criada.
CVE-2016-5216	Um uso depois de gratuito no PDFium no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de um arquivo PDF criado.
CVE-2016-5215	Um uso depois de gratuito em webaudio no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de uma página HTML criada.
CVE-2016-5214	O Google Chrome anterior a 55.0.2883.75 para o Windows manipulou indevidamente os arquivos baixados, o que permitiu a um invasor remoto impedir que o arquivo baixado recebesse a Marca da Web por meio de uma página HTML criada.
CVE-2016-5213	Um uso após o V8 gratuito no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada.
CVE-2016-5212	O Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android insuficientemente higienizava as URLs DevTools, o que permitia que um invasor remoto lesse arquivos locais por meio de uma página HTML criada.
CVE-2016-5211	Um uso depois de gratuito no PDFium no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo PDF criado.
CVE-2016-5210	O estouro de buffer de heap durante a análise de imagem TIFF no PDFium no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo PDF criado.
CVE-2016-5209	A transmissão incorreta na manipulação de bitmap no Blink no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma página HTML criada.
CVE-2016-5208	Pisca no Google Chrome antes de 55.0.2883.75 para Linux e Windows, e 55.0.2883.84 para Android permitiu a possível

Nome	Descrição
	corrupção da árvore DOM durante o tratamento de eventos síncronos, o que permitiu que um invasor remoto injetasse scripts arbitrários ou HTML (UXSS) por meio de um HTML criado página.
CVE-2016-5207	No Blink no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android, a corrupção da árvore DOM poderia ocorrer durante a remoção de um elemento de tela cheia, o que permitia a um invasor remoto executar a execução de código arbitrário através de uma página HTML criada.
CVE-2016-5206	O plug-in PDF no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android seguia incorretamente os redirecionamentos, o que permitia que um invasor remoto ignorasse a Política de mesma origem por meio de uma página HTML criada.
CVE-2016-5205	Pisca no Google Chrome antes de 55.0.2883.75 para Linux, Windows e Mac, lida incorretamente com cargas de páginas adiadas, o que permite que um invasor remoto injete scripts arbitrários ou HTML (UXSS) por meio de uma página HTML criada.
CVE-2016-5204	O vazamento de uma árvore de sombra SVG levando à corrupção da árvore DOM no Blink no Google Chrome antes de 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto injetasse scripts arbitrários ou HTML (UXSS) via uma página HTML criada
CVE-2016-5203	Um uso depois de gratuito no PDFium no Google Chrome anterior a 55.0.2883.75 para Mac, Windows e Linux e 55.0.2883.84 para Android permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de um arquivo PDF criado.
CVE-2016-5201	Um vazamento de privateClass na API de extensões do Google Chrome anterior a 54.0.2840.100 para Linux e 54.0.2840.99 para Windows e 54.0.2840.98 para Mac permitiu que um invasor remoto acessasse o código JavaScript privilegiado por meio de uma página HTML criada.
CVE-2016-5200	V8 no Google Chrome anterior a 54.0.2840.98 para Mac e 54.0.2840.99 para Windows e 54.0.2840.100 para Linux, e 55.0.2883.84 para Android, que aplicava incorretamente regras de tipo, o que permitia que um invasor remoto explorasse potencialmente a corrupção de heap por meio de uma execução Página HTML.
CVE-2016-5199	Um erro de um erro resultando em uma alocação de tamanho zero no FFmpeg no Google Chrome antes de 54.0.2840.98 para Mac e 54.0.2840.99 para Windows e 54.0.2840.100 para Linux, e de 55.0.2883.84 para Android permitiu que um invasor remoto potencialmente explorar corrupção de pilha através de um arquivo de vídeo criado.
CVE-2016-5198	V8 no Google Chrome anterior a 54.0.2840.90 para Linux e 54.0.2840.85 para Android e 54.0.2840.87 para Windows e Mac incluíam pressupostos de otimização incorretos, que permitiam a

Nome	Descrição
	um invasor remoto executar operações arbitrárias de leitura / gravação, levando à execução de código, através de uma página HTML criada.
CVE-2016-5197	O cliente de visualização de conteúdo do Google Chrome anterior a 54.0.2840.85 para Android não tinha URLs de intenção suficientemente validados, o que permitia que um invasor remoto que comprometesse o processo de renderização iniciasse uma atividade arbitrária no sistema por meio de uma página HTML criada.
CVE-2016-5196	O cliente do renderizador de conteúdo do Google Chrome anterior ao 54.0.2840.85 para Android aplicou de maneira insuficiente a Política de mesma origem entre os arquivos baixados, o que permitiu que um invasor remoto acessasse qualquer arquivo baixado e interagisse com sites, incluindo aqueles em que o usuário estava conectado Página HTML.
CVE-2016-5193	O Google Chrome anterior ao 54.0 para iOS não tinha validação suficiente de URLs para janelas abertas pelo DOM, o que permitia que um invasor remoto ignorasse as restrições de navegação para determinados esquemas de URL por meio de páginas HTML criadas.
CVE-2016-5192	Pisca no Google Chrome antes de 54.0.2840.59 para o Windows perdeu uma verificação de CORS no redirecionamento no TextTrackLoader, o que permitiu que um invasor remoto ignorasse as restrições de origem cruzada por meio de páginas HTML criadas.
CVE-2016-5191	Manipulação de marcadores no Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para Android tinha validação insuficiente de dados fornecidos, o que permitia a um invasor remoto injetar scripts arbitrários ou HTML (UXSS) por meio de páginas HTML criadas, como demonstrado por um conflito de interpretação entre userinfo e esquema em uma carga http:// javascript: @ example.com URL.
CVE-2016-5190	Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para o Android tratou incorretamente os ciclos de vida dos objetos durante o desligamento, o que permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de páginas HTML criadas.
CVE-2016-5189	Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para a navegação permitida pelo Android para blob URLs com origens não canônicas, que permitiam que um invasor remoto falsificasse o conteúdo da omnibox (barra de URL) por meio de páginas HTML criadas.
CVE-2016-5188	Vários problemas no Blink no Google Chrome anteriores a 54.0.2840.59 para Windows, Mac e Linux permitem que um invasor remoto falsifique várias partes da interface do usuário do navegador por meio de páginas HTML criadas.
CVE-2016-5187	O Google Chrome anterior ao 54.0.2840.85 para o Android tratou incorretamente a rápida transição para dentro e fora do modo de tela cheia, o que permitiu que um invasor remoto falsificasse o

Nome	Descrição
	conteúdo da omnibox (barra de URL) por meio de páginas HTML criadas.
CVE-2016-5186	Devtools no Google Chrome anterior a 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para o Android manipulou objetos incorretamente após uma falha de tabulação, o que permitiu que um invasor remoto realizasse uma leitura de memória fora dos limites por meio de arquivos PDF criados.
CVE-2016-5185	Pisca no Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para Android incorretamente permitia a reentrada de FrameView :: updateLifecyclePhasesInternal (), que permitia a um atacante remoto realizar uma leitura de memória fora dos limites por meio de páginas HTML criadas.
CVE-2016-5184	PDFium no Google Chrome anterior a 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para o Android tratou incorretamente os ciclos de vida dos objetos em CFFL_FormFillter :: KillFocusForAnnot, o que permitiu que um invasor remoto explorasse potencialmente a corrupção de heap por meio de arquivos PDF criados.
CVE-2016-5183	Um uso de pilha depois de livre no PDFium no Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; O 54.0.2840.85 para Android permite que um invasor remoto explore potencialmente a corrupção de heap por meio de arquivos PDF criados.
CVE-2016-5182	Pisca no Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para o Android não tinha validação suficiente no manuseio de bitmaps, o que permitia que um invasor remoto explorasse potencialmente a corrupção de heap por meio de páginas HTML criadas.
CVE-2016-5181	Pisca no Google Chrome antes de 54.0.2840.59 para Windows, Mac e Linux; 54.0.2840.85 para o Android permitia a execução de microtarefas v8 enquanto o DOM estava em um estado inconsistente, o que permitia que um invasor remoto injetasse scripts arbitrários ou HTML (UXSS) por meio de páginas HTML criadas.
CVE-2016-5178	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 53.0.2785.143 permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-5177	A vulnerabilidade de uso após a liberação no V8 no Google Chrome anterior a 53.0.2785.143 permite que atacantes remotos causem uma negação de serviço (falha) ou possivelmente não tenham outro impacto desconhecido por meio de vetores desconhecidos.
CVE-2016-5176	O Google Chrome anterior a 53.0.2785.113 permite que atacantes remotos contornem o mecanismo de proteção do SafeBrowsing por meio de vetores não especificados.
CVE-2016-5175	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 53.0.2785.113 permitem que invasores causem uma

Nome	Descrição
	negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-5174	O navegador / ui / cocoa / browser_window_controller_private.mm no Google Chrome anterior a 53.0.2785.113 não processa solicitações de tela inteira durante uma transição de tela cheia, o que permite que atacantes remotos causem uma negação de serviço (popup não-suprimido) por meio de um site criado.
CVE-2016-5173	O subsistema de extensões do Google Chrome anterior a 53.0.2785.113 não restringe adequadamente o acesso ao Object.prototype, que permite que atacantes remotos carreguem recursos indesejados e, consequentemente, acionem chamadas de função JavaScript não intencionais e ignorem a Política de mesma origem por meio de um ataque de interceptação indireta.
CVE-2016-5172	O analisador no Google V8, usado no Google Chrome antes de 53.0.2785.113, manipula incorretamente os escopos, o que permite que atacantes remotos obtenham informações confidenciais de locais de memória arbitrária por meio de código JavaScript criado.
CVE-2016-5171	O WebKit / Source / bindings / templates / interface.cpp no Blink, conforme usado no Google Chrome antes de 53.0.2785.113, não impede determinadas chamadas de construtor, o que permite que atacantes remotos causem uma negação de serviço (uso-depois-livre) ou possivelmente não especificou outro impacto por meio de código JavaScript criado.
CVE-2016-5170	O WebKit / Source / bindings / modules / v8 / V8BindingForModules.cpp no Blink, usado no Google Chrome anterior a 53.0.2785.113, não considera adequadamente os efeitos colaterais do getter durante a conversão de chave de matriz, o que permite que atacantes remotos causem uma negação de serviço depois de livre) ou possivelmente não ter especificado outro impacto por meio de chamadas de API criadas pelo Indexed Database (aka IndexedDB).
CVE-2016-5169	A vulnerabilidade de string de formato no Google Chrome OS anterior a 53.0.2785.103 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2016-5168	O Skia, como usado no Google Chrome antes do 50.0.2661.94, permite que atacantes remotos contornem a Política de mesma origem e obtenham informações confidenciais.
CVE-2016-5167	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 53.0.2785.89 no Windows e OS X e anteriores a 53.0.2785.92 no Linux permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-5166	A implementação do download no Google Chrome anterior a 53.0.2785.89 no Windows e no OS X e antes de 53.0.2785.92 no Linux não restringe adequadamente o salvamento de um arquivo:

Nome	Descrição
CVE-2016-5165	// URL referenciado por uma URL http://, o que facilita para o usuário -assistiram atacantes remotos para descobrir hashes NetNTLM e realizar ataques de retransmissão SMB através de uma página da Web criada acessada com a opção de menu "Salvar página como".
CVE-2016-5164	A vulnerabilidade de cross-site scripting (XSS) no subsistema Tools Developer (aka DevTools) no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux permite que invasores remotos injetem script web arbitrário ou HTML através do parâmetro settings em uma string de consulta do URL chrome-devtools-frontend.appspot.com.
CVE-2016-5163	A vulnerabilidade de cross-site scripting (XSS) no WebKit / Source / platform / v8_inspector / V8Debugger.cpp no Blink, usada no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes do 53.0.2785.92 no Linux, permite que atacantes remotos injetem script web arbitrário ou HTML no subsistema Tools Developer (aka DevTools) através de um site criado, conhecido como "Universal XSS (UXSS)".
CVE-2016-5162	A implementação de texto bidirecional no Google Chrome anterior a 53.0.2785.89 no Windows e OS X e anterior a 53.0.2785.92 no Linux não garante a renderização de URLs da esquerda para a direita (LTR), o que permite que atacantes remotos façam falsificações na barra de endereços texto Unicode da direita para a esquerda (RTL), relacionado a omnibox / SuggestionView.java e omnibox / UrlBar.java no Chrome para Android.
CVE-2016-5161	A função AllowCrossRendererResourceLoad em extensions / browser / url_request_util.cc no Google Chrome anterior a 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux não usa adequadamente o campo manifest.json web_accessible_resources de uma extensão para restrições nos elementos IFRAAME, o que torna mais fácil para invasores remotos conduzirem ataques de clickjacking e enganar os usuários para que alterem as configurações de extensão, através de um site criado, uma vulnerabilidade diferente da CVE-2016-5160.
CVE-2016-5160	A função EditingStyle :: mergeStyle no WebKit / Source / core / editing / EditingStyle.cpp no Blink, como usada no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, manipula incorretamente as propriedades personalizadas, o que permite remoto invasores causarem uma negação de serviço ou possivelmente não tenham especificado outro impacto por meio de um site criado que aproveite "tipo de confusão" na classe StylePropertySerializer.
	A função AllowCrossRendererResourceLoad em extensions / browser / url_request_util.cc no Google Chrome anterior a 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux não usa adequadamente o campo manifest.json web_accessible_resources de uma extensão para restrições nos elementos IFRAAME, o que torna mais fácil para invasores remotos

Nome	Descrição
	conduzirem ataques de clickjacking e enganar os usuários para alterar as configurações de extensão, através de um site criado, uma vulnerabilidade diferente da CVE-2016-5162.
CVE-2016-5159	Vários overflows inteiros no OpenJPEG, como usados no PDFium no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes 53.0.2785.92 no Linux, permitem que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente não especificados outro impacto através de dados JPEG 2000 criados que são mal utilizados durante as chamadas opj_aligned_malloc em dwt.c e t1.c.
CVE-2016-5158	Vários overflows de inteiros na função opj_tcd_init_tile em tcd.c em OpenJPEG, conforme usado no PDFium no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, permitem que atacantes remotos causem uma negação de serviço (heap com base no buffer overflow) ou possivelmente ter outro impacto não especificado por meio de dados JPEG 2000 criados.
CVE-2016-5157	O estouro de buffer baseado em heap na função opj_dwt_interleave_v em dwt.c em OpenJPEG, usado no PDFium no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes 53.0.2785.92 no Linux, permite que atacantes remotos executem código arbitrário por meio de coordenadas criadas valores em dados JPEG 2000.
CVE-2016-5156	extensions / renderer / event_bindings.cc nas ligações do evento no Google Chrome anteriores a 53.0.2785.89 no Windows e OS X e anteriores a 53.0.2785.92 no Linux tentam processar eventos filtrados após falha ao adicionar um correspondente de evento, o que permite que atacantes remotos causem negação de serviço (uso após livre) ou possivelmente não ter especificado outro impacto através de vetores desconhecidos.
CVE-2016-5155	O Google Chrome anterior a 53.0.2785.89 no Windows e OS X e anterior a 53.0.2785.92 no Linux não valida corretamente o acesso ao documento inicial, o que permite que atacantes remotos falsifiquem a barra de endereço por meio de um site criado.
CVE-2016-5154	Vários buffer overflows baseados em heap no PDFium, como usados no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um JBig2 imagem.
CVE-2016-5153	A implementação do Web Animations no Blink, como usada no Google Chrome antes do 53.0.2785.89 no Windows e OS X e antes do 53.0.2785.92 no Linux, depende indevidamente da iteração de lista, que permite que atacantes remotos causem uma negação de serviço (use-after- destruição) ou possivelmente não especificou outro impacto através de um site criado.
CVE-2016-5152	O estouro de número inteiro na função opj_tcd_get_decoded_tile_size em tcd.c em OpenJPEG, conforme

Nome	Descrição
CVE-2016-5151	usado no PDFium no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, permite que atacantes remotos causem uma negação de serviço estouro de buffer) ou possivelmente não tenha especificado outro impacto por meio de dados JPEG 2000 criados.
CVE-2016-5150	O PDFium no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux gerencia mishandles timers, o que permite que atacantes remotos causem uma negação de serviço (use-após-free) ou possivelmente não tenham outro impacto por meio de um PDF criado documento, relacionado a fpdfsdk / javascript / JS_Object.cpp e fpdfsdk / javascript / app.cpp.
CVE-2016-5149	WebKit / Source / bindings / modules / v8 / V8BindingForModules.cpp no Blink, como usado no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, tem uma implementação de API do Indexed Database (aka IndexedDB) que não restringir adequadamente a avaliação do caminho do teclado, que permite que atacantes remotos causem uma negação de serviço (uso após livre) ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que aproveita certos efeitos colaterais.
CVE-2016-5149	O subsistema de extensões do Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux depende de uma URL de origem do IFRAME para identificar uma extensão associada, que permite que atacantes remotos realizem ataques de injeção de vinculações de ramal, aproveitando o acesso ao script um recurso que inicialmente tem o about: blank URL.
CVE-2016-5148	A vulnerabilidade de cross-site scripting (XSS) no Blink, usada no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, permite que atacantes remotos injetem scripts web ou HTML arbitrários por meio de vetores relacionados a atualizações de widgets também conhecido como "Universal XSS (UXSS)".
CVE-2016-5147	O Blink, usado no Google Chrome antes de 53.0.2785.89 no Windows e OS X e antes de 53.0.2785.92 no Linux, manipula incorretamente as cargas de páginas adiadas, o que permite que atacantes remotos injetem scripts web ou HTML arbitrários por meio de um site criado, conhecido como "XSS universal". (UXSS). "
CVE-2016-5146	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 52.0.2743.116 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-5145	Piscar, como usado no Google Chrome antes de 52.0.2743.116, não garante que uma propriedade de corrupção seja preservada após uma operação de clone de estrutura em um objeto ImageBitmap derivado de uma imagem de origem cruzada, que

Nome	Descrição
	permite que atacantes remotos contornem a Política de mesma origem por meio de código JavaScript criado.
CVE-2016-5144	O subsistema Developer Tools (aka DevTools) no Blink, usado no Google Chrome antes de 52.0.2743.116, manipula incorretamente o hostname do caminho do script, o parâmetro remoteBase e o parâmetro remoteFrontendUrl, o que permite que atacantes remotos ignorem as restrições de acesso pretendidas por meio de uma URL criada vulnerabilidade diferente de CVE-2016-5143.
CVE-2016-5143	O subsistema Developer Tools (aka DevTools) no Blink, usado no Google Chrome antes de 52.0.2743.116, manipula incorretamente o hostname do caminho do script, o parâmetro remoteBase e o parâmetro remoteFrontendUrl, que permite que atacantes remotos ignorem as restrições de acesso desejadas por meio de uma URL criada vulnerabilidade diferente de CVE-2016-5144.
CVE-2016-5142	A implementação da Web Cryptography API (também conhecida como WebCrypto) no Blink, usada no Google Chrome antes de 52.0.2743.116, não copia adequadamente buffers de dados, o que permite que atacantes remotos causem uma negação de serviço (use-after-free) ou possivelmente não especificados outro impacto por meio de código JavaScript criado, relacionado a NormalizeAlgorithm.cpp e SubtleCrypto.cpp.
CVE-2016-5141	O Blink, usado no Google Chrome antes de 52.0.2743.116, permite que invasores remotos falsifiquem a barra de endereços por meio de vetores envolvendo uma URL provisória para um documento inicialmente vazio, relacionado a FrameLoader.cpp e ScopedPageLoadDeferrer.cpp.
CVE-2016-5140	O estouro de buffer baseado em heap na função opj_j2k_read_SQcd_SQcc em j2k.c no OpenJPEG, como usado no PDFium no Google Chrome antes de 52.0.2743.116, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de dados JPEG 2000 criados.
CVE-2016-5139	Vários overflows inteiros na função opj_tcd_init_tile em tcd.c no OpenJPEG, como usado no PDFium no Google Chrome antes de 52.0.2743.116, permitem que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente tenham outro impacto não especificado por meio de execução Dados JPEG 2000.
CVE-2016-5138	O estouro de número inteiro na função kbasep_vinstr_attach_client no midgard / mali_kbase_vinstr.c no Google Chrome anterior a 52.0.2743.85 permite que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap e uso após livre) aproveitando uma multiplicação irrestrita.
CVE-2016-5137	A função CSPSource :: schemeMatches no WebKit / Source / core / frame / csp / CSPSource.cpp na implementação da Política de segurança de conteúdo (CSP) no Blink, conforme usada no Google Chrome anterior a 52.0.2743.82, não se aplica a http: 80 políticas

Nome	Descrição
CVE-2016-5136	para https: 443 URLs e não se aplica ws: 80 políticas para wss: 443 URLs, o que torna mais fácil para invasores remotos determinar se um site HSTS específico foi visitado lendo um relatório CSP.NOTA: esta vulnerabilidade está associada a uma alteração de especificação após a resolução CVE-2016-1617.
CVE-2016-5135	A vulnerabilidade "usar-depois-livre" no extensions / renderer / user_script_injector.cc no subsistema Extensions do Google Chrome anterior a 52.0.2743.82 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à exclusão do script.
CVE-2016-5135	WebKit / Source / core / html / parser / HTMLPreloadScanner.cpp no Blink, conforme usado no Google Chrome anterior a 52.0.2743.82, não considera informações de critério de referência dentro de um documento HTML durante uma solicitação de pré-carregamento, que permite que atacantes remotos contornem o Conteúdo Mecanismo de proteção da Diretiva de Segurança (CSP) por meio de um site criado, conforme demonstrado por um cabeçalho "Diretiva de Segurança de Conteúdo: origem da origem quando cruzada" que substitui um "<META name = 'referrer' content = 'no- referrer '>" elemento.
CVE-2016-5134	net / proxy / proxy_service.cc no recurso de Configuração automática de proxy (PAC) no Google Chrome anterior a 52.0.2743.82 não garante que as informações de URL sejam restritas a um esquema, host e porta, o que permite que atacantes remotos descubram credenciais operando um servidor com um script PAC, um problema relacionado ao CVE-2016-3763.
CVE-2016-5133	O Google Chrome anterior a 52.0.2743.82 manuseia incorretamente as informações de origem durante a autenticação de proxy, que permite que invasores man-in-the-middle falsifiquem um prompt de login de autenticação de proxy ou açãoem o armazenamento incorreto de credenciais modificando o fluxo de dados do cliente-servidor.
CVE-2016-5132	O subsistema Service Worker no Google Chrome anterior a 52.0.2743.82 não implementa adequadamente a especificação Secure Contexts durante decisões sobre o controle de um subquadro, o que permite que atacantes remotos contornem a Política de mesma origem por meio de um elemento IFRAAME https dentro de um elemento IFRAAME http.
CVE-2016-5131	A vulnerabilidade use-after-free na libxml2 a 2.9.4, como usada no Google Chrome antes de 52.0.2743.82, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores relacionados à função XPointer range-to.
CVE-2016-5130	content / renderer / history_controller.cc no Google Chrome anterior a 52.0.2743.82 não restringe adequadamente vários usos de um método de encaminhamento de JavaScript, o que permite que atacantes remotos falsifiquem a exibição de URL por meio de

Nome	Descrição
um site criado.	
CVE-2016-5129	O Google V8 anterior a 5.2.361.32, usado no Google Chrome anterior a 52.0.2743.82, não processa adequadamente os objetos com corte à esquerda, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou tenham outro impacto não especificado por meio de código JavaScript criado .
CVE-2016-5128	objects.cc no Google V8 anterior a 5.2.361.27, conforme usado no Google Chrome anterior a 52.0.2743.82, não impede que interceptores de API modifiquem um destino de loja sem definir uma propriedade, o que permite que atacantes remotos contornem a Política de mesma origem por meio de uma Web trabalhada local.
CVE-2016-5127	A vulnerabilidade "usar-depois-livre" no WebKit / Source / core / editing / VisibleUnits.cpp no Blink, usada no Google Chrome anterior a 52.0.2743.82, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado envolvendo uma @import at-rule em uma seqüência de token Cascading Style Sheets (CSS) em conjunto com um atributo rel = import de um elemento LINK.
CVE-2016-3679	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.9.385.33, conforme usadas no Google Chrome antes de 49.0.2623.108, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-2845	A implementação da Política de segurança de conteúdo (CSP) no Blink, usada no Google Chrome anterior a 49.0.2623.75, não ignora o componente de caminho de uma URL no caso de uma busca de ServiceWorker, que permite que atacantes remotos obtenham informações confidenciais sobre páginas da Web visitadas lendo Relatórios de violação de CSP, relacionados a FrameFetchContext.cpp e ResourceFetcher.cpp.
CVE-2016-2844	WebKit / Source / core / layout / LayoutBlock.cpp no Blink, conforme usado no Google Chrome antes de 49.0.2623.75, não determina adequadamente quando há invólucros de bloco anônimos, o que permite que atacantes remotos causem uma negação de serviço (conversão incorreta e declaração incorreta) falha) ou possivelmente não ter especificado outro impacto por meio de código JavaScript criado.
CVE-2016-2843	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.9.385.26, conforme usadas no Google Chrome antes de 49.0.2623.75, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-2052	Diversas vulnerabilidades não especificadas no HarfBuzz anteriores à 1.0.6, conforme usadas no Google Chrome antes de 48.05.64.82, permitem que invasores causem uma negação de serviço ou

Nome	Descrição
	possivelmente tenham outro impacto por meio de dados criados, conforme demonstrado por um buffer over-read resultante de um comprimento invertido check in hb-ot-font.cc, um problema diferente do CVE-2015-8947.
CVE-2016-2051	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.8.271.17, conforme usadas no Google Chrome antes de 48.05.64.82, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1711	WebKit / Source / core / loader / FrameLoader.cpp no Blink, como usado no Google Chrome antes de 52.0.2743.82, não desabilita a navegação de quadros durante uma operação de desanexação em um objeto DocumentLoader, que permite que atacantes remotos contornem a Política de mesma origem por meio de um site criado.
CVE-2016-1710	O método ChromeClientImpl :: createWindow no WebKit / Source / web / ChromeClientImpl.cpp no Blink, usado no Google Chrome antes de 52.0.2743.82, não impede a criação de janelas por um quadro adiado, o que permite que atacantes remotos contornem a Política de mesma origem por meio de um site criado.
CVE-2016-1709	O estouro de buffer com base em heap no método ByteArray :: Get em data / byte_array.cc no Google antes de 2016-06-10, conforme usado no Google Chrome antes de 52.0.2743.82, permite que atacantes remotos causem uma negação de serviço ou possivelmente outro impacto não especificado por meio de uma fonte SFNT criada.
CVE-2016-1708	A implementação da instalação sequencial da Chrome Web Store no subsistema Extensions do Google Chrome anterior a 52.0.2743.82 não considera adequadamente a vida útil do objeto durante a observação do progresso, o que permite que atacantes remotos causem uma negação de serviço (use-após-livre) ou possivelmente não especificados outro impacto através de um site criado.
CVE-2016-1707	O ios / web / web_state / ui / crw_web_controller.mm no Google Chrome anterior a 52.0.2743.82 no iOS não garante a substituição de um URL inválido pelo URL about about: blank, que permite que atacantes remotos imitem a exibição do URL por meio de um site criado .
CVE-2016-1706	A implementação de PPAPI no Google Chrome anterior a 52.0.2743.82 não valida a origem de mensagens IPC para o processo de intermediário de plug-in que deveria ter vindo do processo do navegador, o que permite que atacantes remotos ignorem um mecanismo de proteção de caixa de proteção por meio de um tipo de mensagem inesperado broker_process_dispatcher.cc, ppapi_plugin_process_host.cc, ppapi_thread.cc e render_frame_message_filter.cc.
CVE-2016-1705	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 52.0.2743.82 permitem que os invasores causem uma

Nome	Descrição
	negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1704	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 51.0.2704.103 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1703	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 51.0.2704.79 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1702	A função SkRegion :: readFromMemory no core / SkRegion.cpp no Skia, como usada no Google Chrome antes de 51.0.2704.79, não valida a contagem de intervalos, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) via dados serializados criados.
CVE-2016-1701	A implementação do preenchimento automático no Google Chrome antes de 51.0.2704.79 manipula incorretamente a interação entre atualizações de campo e código JavaScript que aciona uma exclusão de quadros, que permite que atacantes remotos causem uma negação de serviço (uso após livre) ou possivelmente outro impacto não especificado por meio de um Web site concebido para o efeito, uma vulnerabilidade diferente da CVE-2016-1690.
CVE-2016-1700	extensions / renderer / runtime_custom_bindings.cc no Google Chrome anterior a 51.0.2704.79 não considera efeitos colaterais durante a criação de uma matriz de exibições de extensão, o que permite que atacantes remotos causem uma negação de serviço (use-após-livre) ou possivelmente tenham outros não especificados impacto através de vetores relacionados a extensões.
CVE-2016-1699	O WebKit / Source / devtools / front_end / devtools.js no subsistema Developer Tools (aka DevTools) no Blink, como usado no Google Chrome antes de 51.0.2704.79, não garante que o parâmetro remoteFrontendUrl esteja associado a um frontend chrome-devtools. URL do appspot.com, que permite que invasores remotos contornem as restrições de acesso desejadas por meio de um URL criado.
CVE-2016-1698	A função createCustomType em extensions / renderer / resources / binding.js nas ligações de extensão no Google Chrome anteriores a 51.0.2704.79 não valida os tipos de módulo, o que pode permitir que invasores carreguem módulos arbitrários ou obtenham informações confidenciais aproveitando uma definição envenenada.
CVE-2016-1697	A função FrameLoader :: startLoad no WebKit / Source / core / loader / FrameLoader.cpp no Blink, como usada no Google Chrome antes de 51.0.2704.79, não impede as navegações de quadros durante as operações de desanexação do DocumentLoader, o que permite que atacantes remotos contornem a mesma origem Política via código JavaScript criado.
CVE-2016-1696	O subsistema de extensões no Google Chrome anterior a

Nome	Descrição
	51.0.2704.79 não restringe adequadamente o acesso de ligações, o que permite que invasores remotos ignorem a Política de mesma origem por meio de vetores não especificados.
CVE-2016-1695	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 51.0.2704.63 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1694	browser / browsing_data / browsing_data_remover.cc no Google Chrome antes de 51.0.2704.63 exclui os pinos HPKP durante a limpeza do cache, o que facilita para invasores remotos falsificar sites por meio de um certificado válido de uma Autoridade de Certificação reconhecida arbitrariamente.
CVE-2016-1693	O navegador / safe_browsing / srt_field_trial_win.cc no Google Chrome anterior a 51.0.2704.63 não usa o serviço HTTPS em dl.google.com para obter a Ferramenta de Remoção de Software, que permite que atacantes remotos falsifiquem o arquivo chrome_cleanup_tool.exe (também conhecido como CCT) por meio de ataque man-in-the-middle em uma sessão HTTP.
CVE-2016-1692	WebKit / Source / core / css / StyleSheetContents.cpp no Blink, como usado no Google Chrome antes de 51.0.2704.63, permite o carregamento entre origens de folhas de estilo CSS por um ServiceWorker mesmo quando o download da folha de estilo tem um tipo MIME incorreto, que permite atacantes remotos para ignorar a Política de mesma origem por meio de um site criado.
CVE-2016-1691	O Skia, usado no Google Chrome antes de 51.0.2704.63, manipula incorretamente execuções de coincidências, o que permite que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente tenham outro impacto não especificado por meio de curvas criadas, relacionadas a SkOpCoincidence.cpp e SkPathOpsCommon .cpp
CVE-2016-1690	A implementação do preenchimento automático no Google Chrome antes de 51.0.2704.63 manipula incorretamente a interação entre atualizações de campo e código JavaScript que aciona uma exclusão de quadros, que permite que invasores remotos causem uma negação de serviço (uso após livre) ou possivelmente outro impacto não especificado por meio de um Web site concebido para o efeito, uma vulnerabilidade diferente da CVE-2016-1701.
CVE-2016-1689	O estouro de buffer com base em heap em content / renderer / media / canvas_capture_handler.cc no Google Chrome anterior a 51.0.2704.63 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um site criado.
CVE-2016-1688	A implementação regexp (expressão regular) no Google V8 anterior a 5.0.71.40, usada no Google Chrome antes de 51.0.2704.63, manipula incorretamente tamanhos de string externos, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) código JavaScript criado.

Nome	Descrição
CVE-2016-1687	A implementação do renderizador no Google Chrome anterior a 51.0.2704.63 não restringe adequadamente a exposição pública de classes, o que permite que atacantes remotos obtenham informações confidenciais por meio de vetores relacionados a extensões.
CVE-2016-1686	A função CPDF_DIBSource :: CreateDecoder no core / fpdfapi / fpdf_render / fpdf_render_loadimage.cpp no PDFium, como usada no Google Chrome antes de 51.0.2704.63, manipula incorretamente a falha de inicialização do decodificador, o que permite que atacantes remotos causem uma negação de serviço (fora de limites lidos) por meio de um documento PDF criado.
CVE-2016-1685	core / fxge / ge / fx_ge_text.cpp no PDFium, como usado no Google Chrome antes de 51.0.2704.63, calcula incorretamente certos valores de índice, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento PDF criado .
CVE-2016-1684	numbers.c na libxslt anterior a 1.1.29, como usado no Google Chrome antes de 51.0.2704.63, manipula incorretamente o token de formato i para xsl: number dados, o que permite que atacantes remotos causem uma negação de serviço (estouro de inteiro ou consumo de recursos) ou possivelmente não especificou outro impacto através de um documento elaborado.
CVE-2016-1683	numbers.c na libxslt anterior a 1.1.29, conforme usado no Google Chrome antes de 51.0.2704.63, manipula incorretamente os nós de namespace, o que permite que atacantes remotos causem uma negação de serviço (acesso à memória heap fora dos limites) ou possivelmente outros impactos não especificados através de um documento elaborado.
CVE-2016-1682	A função ServiceWorkerContainer :: registerServiceWorkerImpl no WebKit / Source / modules / serviceworkers / ServiceWorkerContainer.cpp no Blink, conforme usada no Google Chrome antes de 51.0.2704.63, permite que atacantes remotos contornem o mecanismo de proteção do Content Security Policy (CSP) por meio de um registro do ServiceWorker.
CVE-2016-1681	O estouro de buffer baseado em heap na função opj_j2k_read_SPCod_SPCoc em j2k.c no OpenJPEG, como usado no PDFium no Google Chrome antes de 51.0.2704.63, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento PDF criado.
CVE-2016-1680	A vulnerabilidade use-after-free em ports / SkFontHost_FreeType.cpp no Skia, como usada no Google Chrome antes de 51.0.2704.63, permite que atacantes remotos causem uma negação de serviço (corrupção de memória de heap) ou possivelmente não tenham outro impacto através de vetores desconhecidos.
CVE-2016-1679	A função ToV8Value em content / child /

Nome	Descrição
CVE-2016-1678	v8_value_converter_impl.cc nas vinculações V8 no Google Chrome anteriores a 51.0.2704.63 não restringe adequadamente o uso de getters e setters, o que permite que atacantes remotos causem uma negação de serviço (use-after-free) ou possivelmente não especificou outro impacto através do código JavaScript criado.
CVE-2016-1677	objects.cc no Google V8 anterior a 5.0.71.32, como usado no Google Chrome antes de 51.0.2704.63, não restringe adequadamente a deoptimização lenta, que permite que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente outros não especificados impacto através de código JavaScript criado.
CVE-2016-1677	O uri.js no Google V8 anterior a 5.1.281.26, conforme usado no Google Chrome anterior a 51.0.2704.63, usa um tipo de matriz incorreto, que permite que atacantes remotos obtenham informações confidenciais chamando a função decodeURI e aproveitando a "confusão de tipos".
CVE-2016-1676	extensions / renderer / resources / binding.js nas ligações de extensão no Google Chrome anteriores a 51.0.2704.63 não usa protótipos adequadamente, o que permite que atacantes remotos ignorem a Política de mesma origem por meio de vetores não especificados.
CVE-2016-1675	O Blink, como usado no Google Chrome antes de 51.0.2704.63, permite que atacantes remotos contornem a Política de mesma origem, aproveitando o manuseio incorreto da reconexão do documento durante a destruição, relacionado a FrameLoader.cpp e LocalFrame.cpp.
CVE-2016-1674	O subsistema de extensões no Google Chrome anterior a 51.0.2704.63 permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2016-1673	O Blink, como usado no Google Chrome antes de 51.0.2704.63, permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2016-1672	A função ModuleSystem :: RequireForJsInner em extensions / renderer / module_system.cc nas ligações de extensão no Google Chrome antes de 51.0.2704.63 manuseia incorretamente as propriedades, o que permite que atacantes remotos conduzam ataques de interceptação de ligações e ignorem a Política de mesma origem por meio de vetores não especificados.
CVE-2016-1671	Google Chrome antes de 50.0.2661.102 em Android mishandles / (barra) e \ (barra invertida) caracteres, o que permite que os invasores realizem ataques de passagem de diretórios por meio de um arquivo: URL, relacionado a net / base / escape.cc e net / base / filename_util. cc.
CVE-2016-1670	A condição de corrida na função ResourceDispatcherHostImpl :: BeginRequest em content / browser / loader / resource_dispatcher_host_impl.cc no Google Chrome antes de 50.0.2661.102 permite que atacantes remotos façam solicitações

Nome	Descrição
	HTTP arbitrárias, aproveitando o acesso a um processo de renderizador e reutilizando um ID de solicitação.
CVE-2016-1669	A função Zone :: New em zone.cc no Google V8 anterior a 5.0.71.47, usada no Google Chrome anterior a 50.0.2661.102, não determina adequadamente quando expandir determinadas alocações de memória, o que permite que atacantes remotos causem uma negação de serviço (estouro de buffer) ou possivelmente não ter especificado outro impacto por meio de código JavaScript criado.
CVE-2016-1668	A função forEachForBinding em WebKit / Source / bindings / core / v8 / Iterable.h nas ligações da V8 no Blink, conforme usada no Google Chrome antes de 50.0.2661.102, usa um contexto de criação inadequado, que permite que atacantes remotos ignorem a Política de mesma origem através de um site criado.
CVE-2016-1667	A função TreeScope :: adoptIfNeeded no WebKit / Source / core / dom / TreeScope.cpp na implementação do DOM no Blink, usada no Google Chrome antes de 50.0.2661.102, não impede a execução de scripts durante operações de adoção de nós, o que permite que atacantes remotos para ignorar a Política de mesma origem por meio de um site criado.
CVE-2016-1666	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 50.0.2661.94 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1665	A classe JSGenericLowering no compilador / js-generic-lowering.cc no Google V8, usada no Google Chrome antes de 50.0.2661.94, manipula incorretamente as operadoras de comparação, o que permite que atacantes remotos obtenham informações confidenciais por meio de códigos JavaScript criados.
CVE-2016-1664	A função HistoryController :: UpdateForCommit em content / renderer / history_controller.cc no Google Chrome antes de 50.0.2661.94 manipula incorretamente a interação entre as encaminhamentos de subquadro e outras navegações, o que permite que atacantes remotos falsifiquem a barra de endereços por meio de um site criado.
CVE-2016-1663	A função SerializedScriptValue :: transferArrayBuffers em WebKit / Source / bindings / core / v8 / SerializedScriptValue.cpp nas ligações da V8 no Blink, como usado no Google Chrome antes de 50.0.2661.94, manipula incorretamente certas estruturas de dados de buffer de array, o que permite que atacantes remotos causar uma negação de serviço (usar-após-livre) ou possivelmente ter outro impacto não especificado através de um site criado.
CVE-2016-1662	extensions / renderer / gc_callback.cc no Google Chrome anterior a 50.0.2661.94 não impede a execução de fallback depois que o retorno de chamada do Garbage Collection foi iniciado, o que permite que atacantes remotos causem uma negação de serviço (use-após-free) ou possivelmente outro impacto não especificado

Nome	Descrição
	via vetores desconhecidos.
CVE-2016-1661	Piscar, como usado no Google Chrome antes de 50.0.2661.94, não garante que os quadros satisfaçam a verificação do mesmo processo de renderizador, além de uma verificação de Política de mesma origem, que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente não especificou outro impacto por meio de um site criado, relacionado a BindingSecurity.cpp e DOMWindow.cpp.
CVE-2016-1660	O Blink, usado no Google Chrome antes de 50.0.2661.94, manipula erroneamente as asserções nas classes WTF :: BitArray e WTF :: double_conversion :: Vector, o que permite que atacantes remotos causem uma negação de serviço (gravação fora do limite) ou possivelmente não especificou outro impacto através de um site criado.
CVE-2016-1659	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 50.0.2661.75 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1658	O subsistema de extensões do Google Chrome anterior a 50.0.2661.75 baseia-se incorretamente nas chamadas de método GetOrigin para comparações de origem, o que permite que atacantes remotos contornem a política de mesma origem e obtenham informações confidenciais por meio de uma extensão criada.
CVE-2016-1657	A função WebContentsImpl :: FocusLocationBarByDefault em content / browser / web_contents / web_contents_impl.cc no Google Chrome antes de 50.0.2661.75 mishandles se concentra em determinadas páginas em branco, o que permite que atacantes remotos falsifiquem a barra de endereços por meio de um URL criado.
CVE-2016-1656	A implementação do download no Google Chrome antes do 50.0.2661.75 no Android permite que invasores remotos contornem as restrições de nome de caminho pretendidas por meio de vetores não especificados.
CVE-2016-1655	O Google Chrome anterior a 50.0.2661.75 não considera adequadamente que a remoção de quadros possa ocorrer durante a execução de retorno de chamada, o que permite que atacantes remotos causem uma negação de serviço (uso após livre) ou possivelmente tenham outro impacto não especificado por meio de uma extensão criada.
CVE-2016-1654	O subsistema de mídia do Google Chrome anterior a 50.0.2661.75 não inicializa uma estrutura de dados não especificada, o que permite que atacantes remotos causem uma negação de serviço (operação de leitura inválida) por meio de vetores desconhecidos.
CVE-2016-1653	A implementação do LoadBuffer no Google V8, usada no Google Chrome antes do 50.0.2661.75, manipula incorretamente os tipos de dados, o que permite que atacantes remotos causem uma

Nome	Descrição
	negação de serviço ou possivelmente não tenham outro impacto por meio de código JavaScript criado que dispense uma gravação fora do limite operação, relacionado ao compilador / pipeline.cc e compilador / simplified-lowering.cc.
CVE-2016-1652	A vulnerabilidade de cross-site scripting (XSS) na função ModuleSystem :: RequireForJsInner em extensions / renderer / module_system.cc no subsistema Extensions do Google Chrome antes de 50.0.2661.75 permite que atacantes remotos injetem script web ou HTML arbitrário por meio de um site criado, também conhecido como "Universal XSS (UXSS)".
CVE-2016-1651	O fxcodec / codec / fx_codec_jpx_opj.cpp no PDFium, como usado no Google Chrome antes do 50.0.2661.75, não implementa adequadamente as funções sycc420_to_rgb e sycc422_to_rgb, o que permite que atacantes remotos obtenham informações confidenciais da memória de processo ou causem uma negação de serviço (saída de limites de leitura) por meio de dados JPEG 2000 criados em um documento PDF.
CVE-2016-1650	A função PageCaptureSaveAsMHTMLFunction :: ReturnFailure no navegador / extensions / api / page_capture / page_capture_api.cc no Google Chrome anterior a 49.0.2623.108 permite que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto não especificado ao acionar um erro na criação de um documento MHTML.
CVE-2016-1649	A função Program :: getUniformInternal em Program.cpp em libANGLE, como usado no Google Chrome antes de 49.0.2623.108, não lida corretamente com uma certa incompatibilidade de tipo de dados, que permite que atacantes remotos causem uma negação de serviço (estouro de buffer) ou possivelmente não especificou outro impacto por meio de estágios de shader criados.
CVE-2016-1648	A vulnerabilidade use-after-free na função GetLoadTimes em renderer / loadtimes_extension_bindings.cc na implementação de Extensions no Google Chrome anterior a 49.0.2623.108 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado.
CVE-2016-1647	A vulnerabilidade "usar-depois-livre" na função RenderWidgetHostImpl :: Destroy em content / browser / renderer_host / render_widget_host_impl.cc na implementação de Navegação no Google Chrome antes de 49.0.2623.108 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2016-1646	A implementação de Array.prototype.concat em builtins.cc no Google V8, conforme usada no Google Chrome antes de 49.0.2623.108, não considera adequadamente os tipos de dados de elemento, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) ou possivelmente não especificou outro impacto através do código JavaScript criado.

Nome	Descrição
CVE-2016-1645	Vários erros de sinalização de números inteiros na função opj_j2k_update_image_data em j2k.c no OpenJPEG, conforme usado no PDFium no Google Chrome anterior a 49.0.2623.87, permitem que atacantes remotos causem uma negação de serviço (gravação incorreta e fora-de-limite) ou possivelmente Outro impacto não especificado através de dados JPEG 2000 criados.
CVE-2016-1644	WebKit / Source / core / layout / LayoutObject.cpp no Blink, como usado no Google Chrome antes de 49.0.2623.87, não restringe adequadamente o agendamento de relayout, que permite que atacantes remotos causem uma negação de serviço (use-após-free) ou possivelmente não especificou outro impacto por meio de um documento HTML criado.
CVE-2016-1643	A função ImageInputType :: ensurePrimaryContent no WebKit / Source / core / html / forms / ImageInputType.cpp no Blink, como usado no Google Chrome antes de 49.0.2623.87, não mantém adequadamente o DOM do agente do usuário shadow, que permite que atacantes remotos causem negação de serviço ou, possivelmente, não especificado outro impacto através de vetores que alavancam "tipo de confusão".
CVE-2016-1642	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 49.0.2623.75 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1641	A vulnerabilidade "usar-depois-livre" no conteúdo / browser / web_contents / web_contents_impl.cc no Google Chrome anterior a 49.0.2623.75 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado acionando um download de imagem após uma determinada estrutura de dados ser excluída , como demonstrado por um download favicon.ico.
CVE-2016-1640	A implementação do instalador on-line da Web Store na interface do usuário do Extensions no Google Chrome anterior a 49.0.2623.75 não bloqueia instalações após a exclusão de um quadro de instalação, o que facilita aos invasores fazer com que o usuário acredite que uma solicitação de instalação se originou do usuário próximo destino de navegação por meio de um site criado.
CVE-2016-1639	A vulnerabilidade "usar-depois-de-graça" no navegador / extensões / api / webrtc_audio_private / webrtc_audio_private_api.cc na implementação da API privada de áudio WebRTC no Google Chrome anterior a 49.0.2623.75 permite que invasores remotos causem uma negação de serviço ou possam ter outro impacto não especificado ao usar incorretamente dependência do ponteiro do contexto de recursos.
CVE-2016-1638	extensions / renderer / resources / platform_app.js no subsistema Extensions do Google Chrome anterior a 49.0.2623.75 não restringe adequadamente o uso de APIs da Web, o que permite que atacantes remotos contornem as restrições de acesso pretendidas por meio de um aplicativo de plataforma elaborado.

Nome	Descrição
CVE-2016-1637	A função SkATan2_255 em efeitos / gradientes / SkSweepGradient.cpp no Skia, como usada no Google Chrome antes de 49.0.2623.75, manipula incorretamente cálculos arctangent, que permitem que atacantes remotos obtenham informações confidenciais através de um site criado.
CVE-2016-1636	A função PendingScript :: notifyFinished no WebKit / Source / core / dom / PendingScript.cpp no Google Chrome anterior a 49.0.2623.75 depende de informações de cache de memória sobre ocorrências de verificação de integridade em vez de sucessos de verificação de integridade, o que permite que atacantes remotos ignorem Mecanismo de proteção de integridade de sub-recursos (SRI), acionando duas cargas do mesmo recurso.
CVE-2016-1635	O extensions / renderer / render_frame_observer_natives.cc no Google Chrome anterior a 49.0.2623.75 não considera propriamente as vidas úteis dos objetos e os problemas de reentrada durante o processamento de OnDocumentElementCreated, o que permite que atacantes remotos causem uma negação de serviço (use-após-livre) ou possivelmente não especificados outro impacto através de vetores desconhecidos.
CVE-2016-1634	A vulnerabilidade Use-after-free na função StyleResolver :: appendCSSStyleSheet no WebKit / Source / core / css / resolver / StyleResolver.cpp no Blink, como usada no Google Chrome antes de 49.0.2623.75, permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto por meio de um site criado que aciona a invalidação de estilo CSS (Cascading Style Sheets) durante uma determinada ação de remoção de subárvore.
CVE-2016-1633	A vulnerabilidade de uso após a liberação no Blink, conforme usada no Google Chrome antes de 49.0.2623.75, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2016-1632	O subsistema de extensões do Google Chrome anterior a 49.0.2623.75 não mantém adequadamente propriedades próprias, o que permite que atacantes remotos contornem restrições de acesso pretendidas por meio de código JavaScript criado que aciona uma conversão incorreta, relacionada a extensions / renderer / v8_helpers.h e gin / converter. h.
CVE-2016-1631	A função PPB_Flash_MessageLoop_Impl :: InternalRun em content / renderer / pepper / ppb_flash_message_loop_impl.cc no plug-in do Google Chrome no Google Chrome antes de 49.0.2623.75 manipula incorretamente loops de mensagens aninhadas, o que permite que atacantes remotos contornem a Política de mesma origem por meio de um site criado.
CVE-2016-1630	A função ContainerNode :: parserRemoveChild no WebKit / Source / core / dom / ContainerNode.cpp no Blink, usada no Google Chrome antes de 49.0.2623.75, manipula incorretamente as atualizações de widgets, o que facilita para invasores remotos

Nome	Descrição
CVE-2016-1629	ignorar a Política de mesma origem por meio de um site criado.
CVE-2016-1628	O Google Chrome anterior a 48.0.2564.116 permite que atacantes remotos contornem a mesma política de origem do Blink e um mecanismo de proteção de caixa de proteção por meio de vetores não especificados.
CVE-2016-1628	pi.c no OpenJPEG, como usado no PDFium no Google Chrome antes de 48.0.2564.109, não valida um determinado valor de precisão, que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (leitura fora dos limites) por meio de um imagem JPEG 2000 criada em um documento PDF, relacionada às funções opj_pi_next_rpcl, opj_pi_next_pcrl e opj_pi_next_cprl.
CVE-2016-1627	O subsistema Developer Tools (aka DevTools) no Google Chrome anterior a 48.0.2564.109 não valida os esquemas de URL e garante que o parâmetro remoteBase esteja associado a um URL chrome-devtools-frontend.appspot.com, que permite que atacantes remotos contornem as restrições de acesso pretendidas por meio de uma URL criada, relacionada ao navegador / devtools / devtools_ui_bindings.cc e WebKit / Source / devtools / front_end / Runtime.js.
CVE-2016-1626	A função opj_pi_update_decode_poc em pi.c no OpenJPEG, conforme usada no PDFium no Google Chrome anterior a 48.0.2564.109, calcula incorretamente um determinado valor de índice de camada, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) Documento PDF.
CVE-2016-1625	O recurso Instant do Chrome no Google Chrome anterior a 48.0.2564.109 não garante que um destino de navegação NTP esteja na lista dos mais visitados ou de sugestões, o que permite que atacantes remotos contornem as restrições pretendidas por meio de vetores não especificados relacionados ao serviço instantâneo. cc e search_tab_helper.cc.
CVE-2016-1624	O underflow inteiro na função ProcessCommandsInternal em dec / decode.c no Brotli, como usado no Google Chrome antes de 48.0.2564.109, permite que atacantes remotos causem uma negação de serviço (estouro de buffer) ou possivelmente tenham outro impacto não especificado por meio de dados criados com compactação brotli .
CVE-2016-1623	A implementação do DOM no Google Chrome anterior a 48.0.2564.109 não restringe adequadamente as operações de anexação de quadros durante ou após as operações de desconexão de quadros, o que permite que atacantes remotos contornem a Política de mesma origem por meio de um site criado relacionado a FrameLoader.cpp. HTMLFrameOwnerElement.h, LocalFrame.cpp e WebLocalFrameImpl.cpp.
CVE-2016-1622	O subsistema de extensões do Google Chrome anterior a 48.0.2564.109 não impede o uso do método Object.defineProperty para substituir o comportamento de extensão pretendido, o que

Nome	Descrição
	permite que atacantes remotos contornem a Política de mesma origem por meio de código JavaScript criado.
CVE-2016-1620	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 48.0.2564.82 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2016-1619	Vários transbordamentos de números inteiros nas funções (1) sycc422_to_rgb e (2) sycc444_to_rgb em fxcodec / codec / fx_codec_jpx_opj.cpp no PDFium, como usado no Google Chrome antes de 48.0.2564.82, permitem que atacantes remotos causem uma negação de serviço (fora de limites lidos) ou possivelmente não ter especificado outro impacto por meio de um documento PDF criado.
CVE-2016-1618	O Blink, como usado no Google Chrome antes de 48.05.64.82, não garante que um gerador de números aleatórios cryptographicallyRandomValues seja usado, o que torna mais fácil para os atacantes remotos derrotarem os mecanismos de proteção criptográfica através de vetores não especificados.
CVE-2016-1617	A função CSPSource :: schemeMatches no WebKit / Source / core / frame / csp / CSPSource.cpp na implementação da Política de segurança de conteúdo (CSP) no Blink, conforme usada no Google Chrome antes de 48.0.2564.82, não aplica políticas http a URLs https e não se aplica às políticas ws para URLs, o que torna mais fácil para invasores remotos determinar se um site HSTS específico foi visitado lendo um relatório CSP.
CVE-2016-1616	A função CustomButton :: AcceleratorPressed em ui / views / controls / button / custom_button.cc no Google Chrome anterior a 48.0.2564.82 permite que invasores remotos falsifiquem URLs por meio de vetores que envolvam um botão personalizado sem foco.
CVE-2016-1615	A implementação da omnibox no Google Chrome anterior a 48.0.2564.82 permite que invasores remotos falsifiquem a origem de um documento por meio de vetores não especificados.
CVE-2016-1614	A classe UnacceleratedImageBufferSurface no WebKit / Source / platform / graphics / UnacceleratedImageBufferSurface.cpp no Blink, usada no Google Chrome antes de 48.0.2564.82, manipula incorretamente o modo de inicialização, que permite que atacantes remotos obtenham informações confidenciais da memória do processo por meio de um site criado.
CVE-2016-1613	Várias vulnerabilidades de uso após livre na implementação do formfiller no PDFium, como usadas no Google Chrome antes de 48.05.64.82, permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento PDF criado relacionado ao rastreamento incorreto de a destruição de objetos (1) IPWL_FocusHandler e (2) IPWL_Provider.
CVE-2016-1612	A função LoadIC :: UpdateCaches em ic / ic.cc no Google V8, como usada no Google Chrome antes de 48.0.2564.82, não garante a

Nome	Descrição
	compatibilidade do receptor antes de realizar um lançamento de uma variável não especificada, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente ter outro impacto desconhecido por meio de código JavaScript criado.
CVE-2016-0959	Use após a vulnerabilidade livre no Tempo de Execução do Adobe Flash Player Desktop antes de 20.0.0.267, Liberação do Suporte Estendido do Adobe Flash Player antes de 18.0.0.324, Adobe Flash Player para Google Chrome antes de 20.0.0.267, Adobe Flash Player para Microsoft Edge e Internet Explorer 11 antes de 20.0.0.267, Adobe Flash Player para Internet Explorer 10 e 11 antes de 20.0.0.267, Adobe Flash Player para Linux antes de 11.2.202.559, AIR Desktop Runtime antes de 20.0.0.233, AIR SDK antes de 20.0.0.233, AIR SDK e Compiler antes de 20.0.0.233, AIR for Android antes de 20.0.0.233.
CVE-2015-8664	O estouro de número inteiro na função WebCursor :: Deserialize em conteúdo / common / cursors / webcursor.cc no Google Chrome antes de 47.0.2526.106 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um array de pixels RGBA com dimensões criadas uma vulnerabilidade diferente da CVE-2015-6792.
CVE-2015-8548	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.7.80.23, conforme usadas no Google Chrome antes de 47.0.2526.80, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos, um problema diferente do CVE-2015-8478.
CVE-2015-8480	A função VideoFramePool :: PoolImpl :: CreateFrame em media / base / video_frame_pool.cc no Google Chrome antes de 47.0.2526.73 não inicializa a memória para uma estrutura de dados de quadros de vídeo, o que pode permitir que atacantes remotos causem uma negação de serviço (saída acesso à memória) ou possivelmente não especificou outro impacto, aproveitando a interação incorreta com a função vp3_h_loop_filter_c no libavcodec / vp3dsp.c no FFmpeg.
CVE-2015-8479	A vulnerabilidade use-after-free na função AudioOutputDevice :: OnDeviceAuthorized em media / audio / audio_output_device.cc no Google Chrome antes de 47.0.2526.73 permite que invasores causem uma negação de serviço (corrupção de memória de heap) ou possivelmente não tenham outro impacto acionando o acesso para um dispositivo de saída de áudio não autorizado.
CVE-2015-8478	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.7.80.23, conforme usadas no Google Chrome antes de 47.0.2526.73, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-7834	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.6.85.23, conforme usadas no Google Chrome antes de 46.0.2490.71, permitem que invasores causem uma negação de

Nome	Descrição
	serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-6792	O subsistema MIDI no Google Chrome anterior a 47.0.2526.106 não manipula adequadamente o envio de dados, o que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados, relacionados a midi_manager.cc, midi_manager_alsa.cc e midi_manager_mac.cc, uma vulnerabilidade diferente da CVE-2015-8664.
CVE-2015-6791	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 47.0.2526.80 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-6790	A função WebPageSerializerImpl :: openTagToString no WebKit / Source / web / WebPageSerializerImpl.cpp no serializador de página no Google Chrome anterior a 47.0.2526.80 não usa corretamente entidades HTML, o que pode permitir que atacantes remotos injetem script da Web ou HTML arbitrário por meio de um documento criado , como demonstrado por um caractere de aspas duplas dentro de uma cadeia de aspas simples.
CVE-2015-6789	A condição de corrida na implementação do MutationObserver no Blink, como usada no Google Chrome antes de 47.0.2526.80, permite que atacantes remotos causem uma negação de serviço (use-após-livre) ou possivelmente tenham outro impacto não especificado, aproveitando a exclusão não antecipada de objetos.
CVE-2015-6788	A classe ObjectBackedNativeHandler em extensions / renderer / object_backed_native_handler.cc no subsistema de extensões no Google Chrome antes de 47.0.2526.80 implementa indevidamente funções de manipulador, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que geram "tipo confusão" "
CVE-2015-6787	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 47.0.2526.73 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-6786	A função CSPSourceList :: matches no WebKit / Source / core / frame / csp / CSPSourceList.cpp na implementação da Política de segurança de conteúdo (CSP) no Google Chrome antes de 47.0.2526.73 aceita um blob :, data :, ou sistema de arquivos: URL como um corresponde a um padrão *, que permite que invasores remotos contornem as restrições do esquema desejado em circunstâncias oportunistas, aproveitando uma política que se baseia nesse padrão.
CVE-2015-6785	A função CSPSource :: hostMatches no WebKit / Source / core / frame / csp / CSPSource.cpp na implementação da Política de segurança de conteúdo (CSP) no Google Chrome antes de

Nome	Descrição
CVE-2015-6784	47.0.2526.73 aceita um nome de host xy como uma correspondência para um padrão * .xy, o que pode permitir que atacantes remotos contornem as restrições de acesso pretendidas em circunstâncias oportunistas, aproveitando uma política que se destina a ser específica para subdomínios.
CVE-2015-6783	O serializador de página do Google Chrome anterior a 47.0.2526.73 manuseia incorretamente os comentários da Marca da Web (MOTW) para URLs que contêm uma sequência "-", que pode permitir que atacantes remotos injetem HTML por meio de uma URL criada, conforme demonstrado por um http inicial: /example.com?-- substring.
CVE-2015-6782	A função FindStartOffsetOfFileInZipFile em crazy_linker_zip.cpp em crazy_linker (também conhecida como Crazy Linker) no Android 5.xe 6.x, como usada no Google Chrome antes de 47.0.2526.73, procura indevidamente por um registro EOCD, que permite aos invasores ignorar uma validação de assinatura requisito através de um arquivo ZIP criado.
CVE-2015-6782	A função Document :: open no WebKit / Source / core / dom / Document.cpp no Google Chrome anterior a 47.0.2526.73 não garante que a manipulação de eventos de eliminação de páginas seja compatível com o bloqueio de caixa de diálogo restrita, o que facilita para invasores remotos spoof conteúdo Omnibox através de um site criado.
CVE-2015-6781	O estouro de número inteiro na função FontData :: Bound em data / font_data.cc no Google sfntly, como usado no Google Chrome antes de 47.0.2526.73, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um deslocamento ou comprimento valor dentro de dados de fonte em um contêiner SFNT.
CVE-2015-6780	A vulnerabilidade "usar-depois-livre" na implementação do Infobars no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um site criado relacionado ao navegador / ui / views / website_settings / website_settings_popup_view. cc.
CVE-2015-6779	O PDFium, como usado no Google Chrome antes de 47.0.2526.73, não restringe adequadamente o uso de chrome: URLs, o que permite que atacantes remotos contornem restrições de esquemas pretendidos por meio de um documento PDF criado, conforme demonstrado por um documento com um link para um cromo: // URL de configurações.
CVE-2015-6778	A classe CJBig2_SymbolDict em fxcodec / jbig2 / JBig2_SymbolDict.cpp no PDFium, como usada no Google Chrome antes de 47.0.2526.73, permite que atacantes remotos causem uma negação de serviço (acesso à memória fora do limite) ou possivelmente tenham outro impacto não especificado por meio de um Documento PDF contendo dados criados com compactação JBIG2.

Nome	Descrição
CVE-2015-6777	A vulnerabilidade use-after-free na função ContainerNode :: notifyNodeInsertedInternal no WebKit / Source / core / dom / ContainerNode.cpp na implementação do DOM no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outros não especificados impacto via vetores relacionados a eventos DOMCharacterDataModified para certas inserções de subárvores destacadas.
CVE-2015-6776	As funções opj_dwt_decode_1 * em dwt.c no OpenJPEG, usadas no PDFium no Google Chrome antes de 47.0.2526.73, permitem que atacantes remotos causem uma negação de serviço (acesso a matriz fora do limite) ou possivelmente tenham outro impacto não especificado por meio de JPEG 2000 dados que são mal utilizados durante uma transformada discreta de wavelets.
CVE-2015-6775	fpdfsdk / src / jsapi / fxjs_v8.cpp no PDFium, como usado no Google Chrome antes de 47.0.2526.73, não usa assinaturas, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que alavancam "tipo confusão "
CVE-2015-6774	A vulnerabilidade use-after-free na função GetLoadTimes em renderer / loadtimes_extension_bindings.cc na implementação de Extensions no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que modifique um ponteiro usado para reportar dados do loadTimes.
CVE-2015-6773	A implementação da convolução no Skia, como usada no Google Chrome antes de 47.0.2526.73, não restringe adequadamente os comprimentos de linha, o que permite que atacantes remotos causem uma negação de serviço (acesso à memória fora do limite) ou possivelmente tenham outro impacto não especificado dados gráficos.
CVE-2015-6772	A implementação do DOM no Blink, como usada no Google Chrome antes de 47.0.2526.73, não impede o javascript: navegação de URL enquanto um documento está sendo desanexado, o que permite que atacantes remotos contornem a Política de mesma origem por meio de código JavaScript criado que interaja inadequadamente com um plug-in .
CVE-2015-6771	js / array.js no Google V8, como usado no Google Chrome antes de 47.0.2526.73, implementa incorretamente determinadas operações de mapa e filtro para matrizes, o que permite que atacantes remotos causem uma negação de serviço (acesso à memória fora do limite) ou possivelmente não especificou outro impacto por meio de código JavaScript criado.
CVE-2015-6770	A implementação do DOM no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados, uma vulnerabilidade diferente da CVE-2015-6768.

Nome	Descrição
CVE-2015-6769	A implementação de confirmação de carga provisória no WebKit / Source / bindings / core / v8 / WindowProxy.cpp no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos contornem a Política de mesma origem, aproveitando um atraso na limpeza de proxy de janela.
CVE-2015-6768	A implementação do DOM no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados, uma vulnerabilidade diferente da CVE-2015-6770.
CVE-2015-6767	A vulnerabilidade use-after-free no conteúdo / browser / appcache / appcache_dispatcher_host.cc na implementação do AppCache no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando a manutenção incorreta do ponteiro associada a retornos de chamada.
CVE-2015-6766	A vulnerabilidade de uso após a liberação na implementação do AppCache no Google Chrome antes de 47.0.2526.73 permite que invasores remotos com acesso de representante causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando o comportamento incorreto de AppCacheUpdateJob associado à seleção de cache duplicada.
CVE-2015-6765	A vulnerabilidade "usar-depois-livre" no conteúdo / browser / appcache / appcache_update_job.cc no Google Chrome antes de 47.0.2526.73 permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço, aproveitando a manipulação incorreta de tarefas de atualização do AppCache.
CVE-2015-6764	A função BasicJsonStringifier :: SerializeJSArray em json-stringifier.h no stringifier JSON no Google V8, conforme usada no Google Chrome antes de 47.0.2526.73, carrega impropriamente elementos de matriz, o que permite que atacantes remotos causem uma negação de serviço (fora de limite de acesso à memória) ou possivelmente não tenha especificado outro impacto por meio de código JavaScript criado.
CVE-2015-6763	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 46.0.2490.71 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-6762	A função CSSFontFaceSrcValue :: fetch em core / css / CSSFontFaceSrcValue.cpp na implementação das CSS (Cascading Style Sheets) no Blink, usada no Google Chrome antes de 46.0.2490.71, não usa o algoritmo de solicitação de origem cruzada CORS quando o URL de uma fonte parece ser uma URL de mesma origem, que permite que servidores remotos ignorem a Política de mesma origem por meio de um redirecionamento.
CVE-2015-6761	A função update_dimensions no libavcodec / vp8.c no FFmpeg através do 2.8.1, como usada no Google Chrome antes de 46.0.2490.71 e outros produtos, depende de uma contagem de

Nome	Descrição
	coeficiente de partição durante a operação multiencadeada, que permite que atacantes remotos causem uma negação de serviço (condição de corrida e corrupção de memória) ou possivelmente não ter especificado outro impacto por meio de um arquivo WebM criado.
CVE-2015-6760	A função Image11 :: map em renderer / d3d / d3d11 / Image11.cpp em libANGLE, como usada no Google Chrome antes de 46.0.2490.71, manipula incorretamente as falhas de mapeamento após eventos perdidos pelo dispositivo, o que permite que atacantes remotos causem uma negação de serviço (inválido ler ou escrever) ou possivelmente ter outro impacto não especificado através de vetores envolvendo um dispositivo removido.
CVE-2015-6759	A função shouldTreatAsUniqueOrigin em platform / weborigin / SecurityOrigin.cpp no Blink, como usada no Google Chrome antes de 46.0.2490.71, não garante que a origem de um recurso LocalStorage seja considerada exclusiva, o que permite que atacantes remotos obtenham informações confidenciais por meio de vetores envolvendo um blob: URL.
CVE-2015-6758	A função CPDF_Document :: GetPage em fpdfapi / fpdf_parser / fpdf_parser_document.cpp no PDFium, como usada no Google Chrome antes de 46.0.2490.71, não executa adequadamente um elenco de um objeto de dicionário, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto por meio de um documento PDF criado.
CVE-2015-6757	A vulnerabilidade use-after-free em content / browser / service_worker / embedded_worker_instance.cc na implementação do ServiceWorker no Google Chrome antes de 46.0.2490.71 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado ao potencializar a destruição de objetos em um retorno de chamada.
CVE-2015-6756	A vulnerabilidade use-after-free na implementação de CPDFSDK_PageView em fpdfsdk / src / fsdk_mgr.cpp no PDFium, como usada no Google Chrome antes de 46.0.2490.71, permite que atacantes remotos causem uma negação de serviço (corrupção de memória de heap) ou possivelmente outros não especificados impacto aproveitando o manuseio incorreto de uma anotação focada em um documento PDF.
CVE-2015-6755	A função ContainerNode :: parserInsertBefore no core / dom / ContainerNode.cpp no Blink, como usada no Google Chrome antes de 46.0.2490.71, prossegue com uma inserção de árvore DOM em certos casos em que um nó pai não contém mais um nó filho, o que permite invasores ignorarem a Política de mesma origem por meio de código JavaScript criado.
CVE-2015-6583	O Google Chrome anterior a 45.0.2454.85 não exibe uma barra de localização para a janela de um aplicativo hospedado após a navegação fora do site de instalação, o que pode facilitar a falsificação de conteúdo de atacantes remotos por meio de um

Nome	Descrição
CVE-2015-6582	aplicativo criado, relacionado a browser.cc e hosted_app_browser_controller.cc .
CVE-2015-6582	A função decompor na plataforma / transforma / TransformationMatrix.cpp no Blink, usada no Google Chrome antes de 45.0.2454.85, não verifica se uma inversão de matrizes foi bem-sucedida, o que permite que atacantes remotos causem uma negação de serviço (acesso de memória não inicializado e falha de aplicativo) ou possivelmente não especificou outro impacto através de um site criado.
CVE-2015-6581	Dupla vulnerabilidade livre na função opj_j2k_copy_default_tcp_and_create_tcd em j2k.c no OpenJPEG antes de r3002, como usado no PDFium no Google Chrome antes de 45.0.2454.85, permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória de heap) acionando uma memória falha de alocação.
CVE-2015-6580	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.5.103.29, conforme usadas no Google Chrome antes de 45.0.2454.85, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-5605	A implementação de expressões regulares no Google V8, usada no Google Chrome antes de 44.0.2403.89, manipula indevidamente interrupções, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de código JavaScript criado, conforme demonstrado por um erro na coleta de lixo durante alocação de uma mensagem de exceção de estouro de pilha.
CVE-2015-4491	O estouro de inteiro na função make_filter_table em pixops / pixops.c no gdk-pixbuf anterior a 2.31.5, como usado no Mozilla Firefox antes de 40.0 e no Firefox ESR 38.x antes do 38.2 no Linux, Google Chrome no Linux e outros produtos, permite remoto invasores executem código arbitrário ou causem uma negação de serviço (estouro de buffer baseado em heap e falha de aplicativo) por meio de dimensões de bitmap criadas e manipuladas incorretamente durante o dimensionamento.
CVE-2015-3910	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.3.61.21, conforme usadas no Google Chrome antes de 43.0.2357.65, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-3880	Reducir a vulnerabilidade de redirecionamento no phpBB antes de 3.0.14 e 3.1.x antes do 3.1.4 permite que atacantes remotos redirecionem os usuários do Google Chrome para sites arbitrários e conduzam ataques de phishing por meio de vetores não especificados.
CVE-2015-3336	O Google Chrome anterior a 42.0.2311.90 nem sempre pergunta ao usuário antes de prosseguir com as alterações

Nome	Descrição
CVE-2015-3335	CONTENT_SETTINGS_TYPE_FULLSCREEN e CONTENT_SETTINGS_TYPE_MOUSELOCK, o que permite que invasores remotos assistidos por usuário causem uma negação de serviço (interrupção da interface) ao criar um documento HTML criado contendo código JavaScript com requestFullScreen e requestPointerLock chamadas e organizando o usuário para acessar este documento com um arquivo: URL.
CVE-2015-3334	A função NaClSandbox :: InitializeLayerTwoSandbox nos componentes / nacl / loader / sandbox_linux / nacl_sandbox_linux.cc no Google Chrome antes de 42.0.2311.90 não tem limites RLIMIT_AS e RLIMIT_DATA para os processos Native Client (aka NaCl), o que pode tornar mais fácil para os atacantes remotos realizar ataques de golpe de martelo ou não ter especificado outro impacto, aproveitando a capacidade de executar um programa criado na caixa de proteção NaCl.
CVE-2015-3333	O navegador / ui / website_settings / website_settings.cc no Google Chrome anterior a 42.0.2311.90 nem sempre exibe "Mídia: Permitida por você" em uma tabela Permissões depois que o usuário concedeu permissão de câmera a um site, o que pode facilitar o acesso do usuário - atacantes remotos assistidos para obter dados de vídeo confidenciais do ambiente físico de um dispositivo através de um site criado que liga a câmera no momento em que o usuário acredita que o acesso à câmera é proibido.
CVE-2015-2239	Várias vulnerabilidades não especificadas no Google V8 anteriores a 4.2.77.14, conforme usadas no Google Chrome antes de 42.0.2311.90, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-2238	O Google Chrome anterior a 41.0.2272.76, quando o modo Instant Extended é usado, não considera adequadamente a interação entre os recursos de "pesquisa de 1993" e transições de RELOAD de disco de restauração, o que facilita para invasores remotos falsificar a barra de endereços página de resultados de pesquisa, aproveitando (1) um mecanismo de pesquisa comprometido ou (2) uma vulnerabilidade de XSS em um mecanismo de pesquisa, uma vulnerabilidade diferente da CVE-2015-1231.
CVE-2015-1361	Diversas vulnerabilidades não especificadas no Google V8 anteriores a 4.1.0.21, conforme usadas no Google Chrome antes de 41.0.2272.76, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
	plataforma / image-decoders / ImageFrame.h no Blink, como usado no Google Chrome antes de 40.0.2214.91, não inicializa uma variável que é usada em chamadas para a função Skia SkBitmap :: setAlphaType, que pode permitir que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto através de um documento HTML criado,

Nome	Descrição
CVE-2015-1360	uma vulnerabilidade diferente da CVE-2015-1205.
CVE-2015-1359	O Skia, como usado no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço (buffer over-read) ou possivelmente não tenham outro impacto através de dados criados incorretamente durante o desenho do texto, relacionado ao gpu / GrBitmapTextContext.cpp e gpu / GrDistanceFieldTextContext.cpp, uma vulnerabilidade diferente da CVE-2015-1205.
CVE-2015-1359	Vários erros off-one em fpdfapi / fpdf_font / font_int.h no PDFium, como usado no Google Chrome antes de 40.0.2214.91, permitem que atacantes remotos causem uma negação de serviço (estouro de buffer) ou possivelmente tenham outro impacto não especificado por meio de um trabalho Documento PDF, relacionado a um problema de "estouro intra-objeto", uma vulnerabilidade diferente da CVE-2015-1205.
CVE-2015-1346	Várias vulnerabilidades não especificadas no Google V8 antes de 3.30.33.15, conforme usadas no Google Chrome antes de 40.0.2214.91, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1304	object-observe.js no Google V8, como usado no Google Chrome antes de 45.0.2454.101, não restringe adequadamente as chamadas de método nos objetos de verificação de acesso, o que permite que atacantes remotos contornem a Política de mesma origem por meio de (1) observe ou (2) chamada getNotifier.
CVE-2015-1303	bindings / core / v8 / V8DOMWrapper.h no Blink, como usado no Google Chrome antes de 45.0.2454.101, não realiza uma ação de relançamento para propagar informações sobre uma exceção de contexto cruzado, que permite que atacantes remotos contornem a Política de mesma origem por meio de um documento HTML criado contendo um elemento IFRAME.
CVE-2015-1302	O visualizador de PDF do Google Chrome anterior a 46.0.2490.86 não restringe adequadamente as mensagens de script e a exposição da API, o que permite que atacantes remotos contornem a Política de mesma origem por meio de um encaixe não intencional ou plug-in não intencional relacionado a pdf.js e out_of_process_instance.cc.
CVE-2015-1301	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 45.0.2454.85 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1300	A função FrameFetchContext :: updateTimingInfoForIFrameNavigation no core / loader / FrameFetchContext.cpp no Blink, conforme usada no Google Chrome antes de 45.0.2454.85, não restringe adequadamente a disponibilidade dos tempos da API de tempo de recursos do IFRAME, o que permite que atacantes remotos obtenham

Nome	Descrição
CVE-2015-1299	informações confidenciais por meio de Código JavaScript que aproveita uma chamada histórica.
CVE-2015-1298	A vulnerabilidade "use-after-free" na implementação do temporizador compartilhado no Blink, usada no Google Chrome antes de 45.0.2454.85, permite que atacantes remotos causem uma negação de serviço ou possivelmente outro impacto não especificado, aproveitando o disparo incorreto do timer relacionado a ThreadTimers. cpp e Timer.cpp.
CVE-2015-1298	A função RuntimeEventRouter :: OnExtensionUninstalled em extensões / browser / api / runtime / runtime_api.cc no Google Chrome anterior a 45.0.2454.85 não garante que a preferência setUninstallURL corresponda ao URL de um site, o que permite que os atacantes remotos assistidos pelo usuário acessem a um URL arbitrário por meio de uma extensão criada que é desinstalada.
CVE-2015-1297	A implementação da API WebRequest nas extensões / browser / api / web_request / web_request_api.cc no Google Chrome antes de 45.0.2454.85 não considera adequadamente a fonte de uma solicitação antes de aceitar a solicitação, o que permite que atacantes remotos contornem as restrições de acesso pretendidas app ou (2) extensão.
CVE-2015-1296	A implementação de UnescapeURLWithAdjustmentsImpl em net / base / escape.cc no Google Chrome anterior a 45.0.2454.85 não impede a exibição de caracteres Unicode LOCK na omnibox, o que facilita para invasores remotos falsificar o ícone de bloqueio SSL colocando um desses caracteres em o fim de um URL, conforme demonstrado pela omnibox em localizações de idiomas escritos da direita para a esquerda.
CVE-2015-1295	Várias vulnerabilidades de uso após a liberação na classe PrintWebViewHelper em components / printing / renderer / print_web_view_helper.cc no Google Chrome anteriores a 45.0.2454.85 permitem que invasores remotos assistidos por usuário causem uma negação de serviço ou possivelmente tenham outro impacto não especificado acionando o IPC aninhado durante a preparação para impressão, conforme demonstrado por mensagens associadas a documentos PDF em conjunto com mensagens sobre recursos da impressora.
CVE-2015-1294	A vulnerabilidade use-after-free na função SkMatrix :: invertNonIdentity no core / SkMatrix.cpp no Skia, como usada no Google Chrome antes de 45.0.2454.85, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado ao acionar o uso de elementos de matriz que levam a um resultado infinito durante um cálculo de inversão.
CVE-2015-1293	A implementação do DOM no Blink, conforme usada no Google Chrome antes de 45.0.2454.85, permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.

Nome	Descrição
CVE-2015-1292	A função <code>NavigatorServiceWorker :: serviceWorker</code> em <code>modules / serviceworkers / NavigatorServiceWorker.cpp</code> no Blink, conforme usada no Google Chrome antes de 45.0.2454.85, permite que atacantes remotos contornem a Política de mesma origem acessando um Service Worker.
CVE-2015-1291	A função <code>ContainerNode :: parserRemoveChild</code> no <code>core / dom / ContainerNode.cpp</code> no Blink, conforme usada no Google Chrome antes de 45.0.2454.85, não verifica se um nó é esperado, o que permite que atacantes remotos contornem a Política de mesma origem ou causem uma negação de serviço (corrupção de árvore DOM) através de um site com código JavaScript criado e elementos IFRAME.
CVE-2015-1290	O mecanismo do Google V8, usado no Google Chrome antes de 44.0.2403.89 e no QtWebEngineCore no Qt antes do 5.5.1, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou executem código arbitrário por meio de um site criado.
CVE-2015-1289	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 44.0.2403.89 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1288	A implementação da Spellcheck API no Google Chrome anterior a 44.0.2403.89 não usa uma sessão HTTPS para fazer o download de um dicionário Hunspell, que permite que invasores man-in-the-middle forneçam sugestões de ortografia incorretas ou possivelmente tenham outro impacto não especificado por meio de um arquivo criado questão relacionada ao CVE-2015-1263.
CVE-2015-1287	O Blink, usado no Google Chrome antes de 44.0.2403.89, permite uma exceção no modo quirks que limita os casos em que um documento CSS (Cascading Style Sheets) é necessário para ter o tipo de conteúdo <code>text / css</code> , o que permite que atacantes remotos ignorem a mesma política de origem por meio de um site criado, relacionado ao <code>core / fetch / CSSStyleSheetResource.cpp</code> .
CVE-2015-1286	A vulnerabilidade de cross-site scripting (XSS) na função <code>V8ContextNativeHandler :: GetModuleSystem</code> em <code>extensions / renderer / v8_context_native_handler.cc</code> no Google Chrome antes de 44.0.2403.89 permite que invasores remotos injetem scripts da Web ou HTML arbitrários aproveitando a falta de uma determinada restrição de contexto V8 , também conhecido como Blink "Universal XSS (UXSS)".
CVE-2015-1285	A função <code>XSSAuditor :: canonicalize</code> no <code>core / html / parser / XSSAuditor.cpp</code> no <code>auditor XSS</code> no Blink, conforme usada no Google Chrome antes de 44.0.2403.89, não escolhe adequadamente um ponto de truncamento, o que facilita a obtenção de invasores remotos informações sensíveis através de um ataque de tempo linear não especificado.
CVE-2015-1284	A função <code>LocalFrame :: isURLAllowed</code> em <code>core / frame / LocalFrame.cpp</code> no Blink, conforme usada no Google Chrome antes de 44.0.2403.89, não escolhe adequadamente um ponto de truncamento, o que facilita a obtenção de invasores remotos informações sensíveis através de um ataque de tempo linear não especificado.

Nome	Descrição
	<p>LocalFrame.cpp no Blink, conforme usada no Google Chrome antes de 44.0.2403.89, não verifica adequadamente o número máximo de quadros de uma página, o que permite que atacantes remotos causem uma negação de serviço (valor de contagem inválido e use-após-livre) ou possivelmente não tenha especificado outro impacto por meio de código JavaScript criado que faça muitas chamadas createElement para elementos IFRAME.</p>
CVE-2015-1283	<p>Vários transbordamentos de números inteiros na função XML_GetBuffer em Expat até 2.1.0, conforme usado no Google Chrome antes de 44.0.2403.89 e outros produtos, permitem que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente tenham outro impacto não especificado via Dados XML criados, um problema relacionado ao CVE-2015-2716.</p>
CVE-2015-1282	<p>Várias vulnerabilidades de uso após livre em fpdfsdk / src / javascript / Document.cpp no PDFium, usadas no Google Chrome antes de 44.0.2403.89, permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento PDF criado , relacionado às funções (1) Document :: delay e (2) Document :: DoFieldDelay.</p>
CVE-2015-1281	<p>core / loader / ImageLoader.cpp no Blink, como usado no Google Chrome antes de 44.0.2403.89, não determina adequadamente o contexto V8 de uma microtarefa, que permite que atacantes remotos contornem as restrições da Diretiva de Segurança de Conteúdo (CSP), fornecendo uma imagem de um fonte não intencional.</p>
CVE-2015-1280	<p>SkPictureShader.cpp no Skia, como usado no Google Chrome antes de 44.0.2403.89, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado, aproveitando o acesso a um processo de renderizador e fornecendo dados serializados criados.</p>
CVE-2015-1279	<p>O estouro de número inteiro na função CJBig2_Image :: expand em fxcodec / jbig2 / JBig2_Image.cpp no PDFium, como usado no Google Chrome antes de 44.0.2403.89, permite que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente não especificados outro impacto através de grandes valores de altura e passada.</p>
CVE-2015-1278	<p>content / browser / web_contents / web_contents_impl.cc no Google Chrome anterior a 44.0.2403.89 não garante que a caixa de diálogo modal de um documento PDF seja fechada durante a navegação para uma página intersticial, o que permite que invasores remotos falsifiquem URLs por meio de um documento criado, conforme demonstrado pelo documento alert_dialog.pdf.</p>
CVE-2015-1277	<p>A vulnerabilidade "usar-depois-livre" na implementação de acessibilidade no Google Chrome antes de 44.0.2403.89 permite que invasores remotos causem uma negação de serviço ou</p>

Nome	Descrição
	possivelmente tenham outro impacto não especificado, aproveitando a falta de determinadas verificações de validade para estruturas de dados de árvore de acessibilidade.
CVE-2015-1276	A vulnerabilidade use-after-free em content / browser / indexed_db / indexed_db_backing_store.cc na implementação do IndexedDB no Google Chrome antes de 44.0.2403.89 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando uma ação de aborto antes de um certo escrever operação.
CVE-2015-1275	A vulnerabilidade de cross-site scripting (XSS) em org / chromium / chrome / browser / UrlUtilities.java no Google Chrome antes de 44.0.2403.89 no Android permite que invasores remotos injetem scripts da Web ou HTML arbitrários por meio de uma intenção criada: URL, conforme demonstrado por um alerta de fuga (document.cookie); // substring, também conhecido como "Universal XSS (UXSS)".
CVE-2015-1274	O Google Chrome anterior a 44.0.2403.89 não garante que a lista de abertura automática omita todos os tipos de arquivo perigosos, o que facilita a execução de código arbitrário por invasores remotos, fornecendo um arquivo criado e aproveitando os "arquivos sempre abertos deste usuário" anteriores de um usuário escolha, relacionado a download_commands.cc e download_prefs.cc.
CVE-2015-1273	O estouro de buffer baseado em heap em j2k.c no OpenJPEG antes de r3002, usado no PDFium no Google Chrome antes de 44.0.2403.89, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de dados JPEG2000 inválidos em um documento PDF.
CVE-2015-1272	A vulnerabilidade "usar-depois-livre" na implementação do processo de GPU no Google Chrome antes de 44.0.2403.89 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado aproveitando a disponibilidade contínua de uma estrutura de dados GPUChannelHost durante o desligamento do Blink, relacionado ao conteúdo /browser/gpu/browser_gpu_channel_host_factory.cc e content / renderer / render_thread_impl.cc.
CVE-2015-1271	O PDFium, como usado no Google Chrome antes de 44.0.2403.89, não lida corretamente com certas condições de falta de memória, o que permite que atacantes remotos causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente tenham outro impacto não especificado Documento PDF que aciona uma grande alocação de memória.
CVE-2015-1270	A função ucnv_io_getConverterName em comum / ucnv_io.cpp em Componentes Internacionais para Unicode (ICU), usada no Google Chrome antes de 44.0.2403.89, manipula incorretamente nomes de conversores com x-substrings iniciais, o que permite que

Nome	Descrição
	atacantes remotos causem uma negação de serviço (leia-se memória não inicializada) ou possivelmente não especificou outro impacto por meio de um arquivo criado.
CVE-2015-1269	A função DecodeHSTSPreloadRaw em net / http / transport_security_state.cc no Google Chrome antes de 43.0.2357.130 não canoniza corretamente nomes de host DNS antes de fazer comparações com entradas de pré-carregamento HSTS ou HPKP, o que permite que atacantes remotos contornem restrições de acesso desejadas por meio de uma string que (1) termina em um. (ponto) ou (2) não é totalmente minúscula.
CVE-2015-1268	bindings / scripts / v8_types.py no Blink, conforme usado no Google Chrome antes de 43.0.2357.130, não seleciona adequadamente um contexto de criação para o wrapper DOM de um valor de retorno, que permite que atacantes remotos contornem a Política de mesma origem por código JavaScript criado, demonstrado pelo uso de um dado: URL.
CVE-2015-1267	O Blink, como usado no Google Chrome antes de 43.0.2357.130, não restringe adequadamente o contexto de criação durante a criação de um wrapper DOM, que permite que atacantes remotos contornem a Política de mesma origem por meio de código JavaScript criado que usa uma API pública Blink relacionada a WebArrayBufferConverter .cpp, WebBlob.cpp, WebDOMError.cpp e WebDOMFileSystem.cpp.
CVE-2015-1266	content / browser / webui / content_web_ui_controller_factory.cc no Google Chrome antes de 43.0.2357.130 não considera adequadamente o esquema para determinar se um URL está associado a um WebUI SiteInstance, que permite que atacantes remotos contornem restrições de acesso pretendidas por meio de um URL semelhante, conforme demonstrado pelo uso de http://gpu quando há uma classe WebUI para manipular solicitações chrome://gpu.
CVE-2015-1265	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 43.0.2357.65 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1264	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome anterior a 43.0.2357.65 permite que invasores remotos assistidos por usuário injetem scripts da Web ou HTML arbitrários por meio de dados criados incorretamente pelo recurso Marcadores.
CVE-2015-1263	A implementação da Spellcheck API no Google Chrome anterior a 43.0.2357.65 não usa uma sessão HTTPS para fazer o download de um dicionário Hunspell, que permite que invasores man-in-the-middle forneçam sugestões de ortografia incorretas ou possivelmente tenham outro impacto não especificado por meio de um arquivo criado.
CVE-2015-1262	platform / fonts / shaping / HarfBuzzShaper.cpp no Blink, como usado no Google Chrome antes de 43.0.2357.65, não inicializa um

Nome	Descrição
	determinado campo de largura, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de texto Unicode criado .
CVE-2015-1261	O Android / java / src / org / cromo / chrome / browser / WebsiteSettingsPopup.java no Google Chrome antes de 43.0.2357.65 no Android não restringe adequadamente o uso do identificador de fragmento de um URL durante a construção de um pop-up de informações de página, que permite que atacantes remotos falsifiquem a barra de URL ou forneçam conteúdo pop-up enganoso por meio de texto criado.
CVE-2015-1260	Várias vulnerabilidades de uso após a liberação no conteúdo / renderizador / mídia / user_media_client_impl.cc na implementação WebRTC no Google Chrome antes de 43.0.2357.65 permitem que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que seja executado após conclusão de um pedido getUserMedia.
CVE-2015-1259	O PDFium, como usado no Google Chrome antes de 43.0.2357.65, não inicializa adequadamente a memória, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2015-1258	O Google Chrome anterior a 43.0.2357.65 depende do código libvpx que não foi criado com um valor adequado de limite de tamanho, que permite que atacantes remotos açãoem um valor negativo para um campo de tamanho e, consequentemente, causem uma negação de serviço ou possivelmente outros não especificados. impacto, através de um tamanho de quadro criado em dados de vídeo VP9.
CVE-2015-1257	platform / graphics / filters / FECColorMatrix.cpp na implementação do SVG no Blink, como usado no Google Chrome antes de 43.0.2357.65, não manipula adequadamente um número insuficiente de valores em um filtro feColorMatrix, que permite que atacantes remotos causem uma negação de serviço (estouro de contêiner) ou possivelmente não ter especificado outro impacto por meio de um documento criado.
CVE-2015-1256	A vulnerabilidade "usar-depois-livre" na implementação do SVG no Blink, usada no Google Chrome antes de 43.0.2357.65, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento elaborado que aproveita o manuseio inadequado de uma árvore de sombra para um elemento de uso.
CVE-2015-1255	A vulnerabilidade use-after-free no conteúdo / renderer / media / webaudio_capturer_source.cc na implementação do WebAudio no Google Chrome antes de 43.0.2357.65 permite que invasores remotos causem uma negação de serviço (corrupção de memória de heap) ou possivelmente tenham outro impacto não especificado ao aproveitar manipulação de uma ação de parada para uma faixa

Nome	Descrição
	de áudio.
CVE-2015-1254	core / dom / Document.cpp no Blink, conforme usado no Google Chrome antes de 43.0.2357.65, ativa a herança do atributo designMode, que permite que atacantes remotos contornem a Política de mesma origem, aproveitando a disponibilidade da edição.
CVE-2015-1253	core / html / parser / HTMLConstructionSite.cpp na implementação do DOM no Blink, como usado no Google Chrome antes de 43.0.2357.65, permite que atacantes remotos contornem a Política de mesma origem por meio de código JavaScript criado que acrescenta um filho a um elemento SCRIPT, relacionado a as funções insert e executeReparentTask.
CVE-2015-1252	common / partial_circular_buffer.cc no Google Chrome antes de 43.0.2357.65 não manipula corretamente os envoltórios, o que permite que atacantes remotos contornem um mecanismo de proteção de sandbox ou causem uma negação de serviço (gravação fora dos limites) por meio de vetores que acionam uma operação de gravação com uma grande quantidade de dados, relacionados às funções PartialCircularBuffer :: Write e PartialCircularBuffer :: DoWrite.
CVE-2015-1251	A vulnerabilidade use-after-free na implementação do SpeechRecognitionClient no subsistema Speech no Google Chrome antes de 43.0.2357.65 permite que atacantes remotos executem código arbitrário por meio de um documento criado.
CVE-2015-1250	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 42.0.2311.135 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1249	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 42.0.2311.90 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1248	A API FileSystem no Google Chrome anterior a 40.0.2214.91 permite que atacantes remotos contornem o mecanismo de proteção SafeBrowsing for Arquivos Executáveis criando um arquivo .exe em um sistema de arquivos temporário e fazendo referência a esse arquivo com um sistema de arquivos: http: URL.
CVE-2015-1247	A função SearchEngineTabHelper :: OnPageHasOSDD no navegador / ui / search_engines / search_engine_tab_helper.cc no Google Chrome anterior a 42.0.2311.90 não impede o uso de um arquivo: URL para um documento XML do descriptor OpenSearch, que pode permitir que atacantes remotos obtenham informações confidenciais de locais arquivos por meio de um site http (ou 2) https criado (1).
CVE-2015-1246	O Blink, conforme usado no Google Chrome antes de 42.0.2311.90, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores

Nome	Descrição
	não especificados.
CVE-2015-1245	A vulnerabilidade use-after-free na função OpenPDFInReaderView :: Update no navegador / ui / views / location_bar / open_pdf_in_reader_view.cc no Google Chrome antes de 41.0.2272.76 pode permitir que atacantes remotos assistidos por usuários causem uma negação de serviço (corrupção de memória de heap) ou possivelmente não especificou outro impacto ao acionar a interação com um botão "Abrir PDF no Reader" do PDFium que possui uma associação de guias inválida.
CVE-2015-1244	A função URLRequest :: GetHSTSRedirect em url_request / url_request.cc no Google Chrome anterior a 42.0.2311.90 não substitui o esquema ws pelo esquema wss sempre que uma Política HSTS estiver ativa, o que facilita para os invasores remotos obter informações confidenciais ao farejarem a rede para tráfego WebSocket.
CVE-2015-1243	A vulnerabilidade use-after-free na função MutationObserver :: disconnect no core / dom / MutationObserver.cpp na implementação do DOM no Blink, como usada no Google Chrome antes de 42.0.2311.135, permite que atacantes remotos causem uma negação de serviço ou possivelmente Outro impacto não especificado, disparando uma tentativa de cancelar o registro de um objeto MutationObserver que não está registrado no momento.
CVE-2015-1242	A função ReduceTransitionElementsKind em hydrogen-check-elimination.cc no Google V8 anterior a 4.2.77.8, conforme usada no Google Chrome antes de 42.0.2311.90, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que aproveita "tipo confusão" na otimização de seleção-eliminação.
CVE-2015-1241	O Google Chrome anterior a 42.0.2311.90 não considera adequadamente a interação da navegação de página com o gerenciamento de eventos de toque e eventos de gesto, o que permite que atacantes remotos açãoem ações de interface do usuário não intencionais por meio de um site criado por um ataque "tapjacking".
CVE-2015-1240	O gpu / blink / webgraphicscontext3d_impl.cc na implementação do WebGL no Google Chrome antes de 42.0.2311.90 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de um programa WebGL criado que açãoe uma inconsistência de estado.
CVE-2015-1239	A dupla vulnerabilidade livre na função j2k_read_ppm_v3 no OpenJPEG antes de r2997, como usada no PDFium no Google Chrome, permite que atacantes remotos causem uma negação de serviço (falha de processo) por meio de um PDF criado.
CVE-2015-1238	O Skia, como usado no Google Chrome antes de 42.0.2311.90, permite que atacantes remotos causem uma negação de serviço (gravação fora do limite) ou possivelmente tenham outro impacto

Nome	Descrição
	não especificado por meio de vetores desconhecidos.
CVE-2015-1237	A vulnerabilidade usar-depois-livre na função RenderFrameImpl :: OnMessageReceived em content / renderer / render_frame_impl.cc no Google Chrome antes de 42.0.2311.90 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam mensagens IPC de renderização durante uma operação de separação.
CVE-2015-1236	A função MediaElementAudioSourceNode :: process em modules / webaudio / MediaElementAudioSourceNode.cpp na implementação da Web Audio API no Blink, usada no Google Chrome antes de 42.0.2311.90, permite que atacantes remotos contornem a Política de mesma origem e obtenham valores de amostra de áudio sensíveis por meio de um Web Site criado contendo um elemento de mídia.
CVE-2015-1235	A função ContainerNode :: parserRemoveChild no core / dom / ContainerNode.cpp no analisador HTML no Blink, conforme usada no Google Chrome antes de 42.0.2311.90, permite que atacantes remotos contornem a Política de mesma origem por meio de um documento HTML criado com um elemento IFRAME.
CVE-2015-1234	A condição de corrida em gpu / command_buffer / service / gles2_cmd_decoder.cc no Google Chrome anterior a 41.0.2272.118 permite que atacantes remotos causem uma negação de serviço (estouro de buffer) ou possivelmente tenham outro impacto não especificado manipulando comandos OpenGL ES.
CVE-2015-1233	O Google Chrome anterior a 41.0.2272.118 não lida adequadamente com a interação entre o IPC, a API do Gamepad e o Google V8, que permite que atacantes remotos executem código arbitrário por meio de vetores não especificados.
CVE-2015-1232	O erro de índice de matriz na função MidiManagerUsb :: DispatchSendMidiData em media / midi / midi_manager_usb.cc no Google Chrome antes de 41.0.2272.76 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando o acesso do renderizador para fornecer um índice de porta inválido que aciona uma operação de gravação fora dos limites, uma vulnerabilidade diferente da CVE-2015-1212.
CVE-2015-1231	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 41.0.2272.76 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1230	A função getHiddenProperty em bindings / core / v8 / V8EventListenerList.h no Blink, conforme usada no Google Chrome antes de 41.0.2272.76, tem um conflito de nome com a classe AudioContext, que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outros não especificados. impacto via código JavaScript que adiciona um

Nome	Descrição
CVE-2015-1229	ouvinte de evento AudioContext e dispara "confusão de tipo".
CVE-2015-1228	net / http / proxy_client_socket.cc no Google Chrome antes de 41.0.2272.76 não manipula adequadamente um código de status HTTP 407 (também conhecido como Proxy Authentication Required) acompanhado por um cabeçalho Set-Cookie, que permite que servidores proxy remotos realizem ataques de injeção de cookie por meio de um resposta trabalhada.
CVE-2015-1228	A função RenderCounter :: updateCounter em core / rendering / RenderCounter.cpp no Blink, como usada no Google Chrome antes de 41.0.2272.76, não força uma operação de relayout e consequentemente não inicializa memória para uma estrutura de dados, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente não ter especificado outro impacto por meio de uma sequência de token de CSS (Cascading Style Sheets) criada.
CVE-2015-1227	A função DragImage :: create na plataforma / DragImage.cpp no Blink, como usada no Google Chrome antes de 41.0.2272.76, não inicializa a memória para o desenho da imagem, o que permite que invasores remotos tenham um impacto não especificado acionando uma decodificação de imagem com falha, como demonstrado por uma imagem para a qual a orientação padrão não pode ser usada.
CVE-2015-1226	A função DebuggerFunction :: InitAgentHost no navegador / extensions / api / debugger / debugger_api.cc no Google Chrome anterior a 41.0.2272.76 não restringe adequadamente quais URLs estão disponíveis como destinos de depuração, o que permite que atacantes remotos contornem restrições de acesso pretendidas por meio de uma extensão criada .
CVE-2015-1225	O PDFium, usado no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2015-1224	A função VpxVideoDecoder :: VpxDecode em media / filters / vpx_video_decoder.cc na implementação do vpxdecoder no Google Chrome anterior a 41.0.2272.76 não garante que as dimensões do plano alfa sejam idênticas às dimensões da imagem, o que permite que atacantes remotos causem uma negação de serviço (fora dos limites lidos) por meio de dados de vídeo VPx criados.
CVE-2015-1223	Várias vulnerabilidades de uso após a liberação no core / html / HTMLInputElement.cpp na implementação do DOM no Blink, conforme usadas no Google Chrome antes de 41.0.2272.76, permitem que atacantes remotos causem uma negação de serviço ou possivelmente não tenham outro impacto por meio de vetores Acione eventos de alteração estranhos, conforme demonstrado por eventos para entrada inválida ou entrada para campos somente leitura, relacionados às funções initializeTypeInParsing e updateType.
CVE-2015-1222	Diversas vulnerabilidades de uso após a atualização na implementação de ServiceWorkerScriptCacheMap no conteúdo /

Nome	Descrição
CVE-2015-1221	browser / service_worker / service_worker_script_cache_map.cc no Google Chrome antes de 41.0.2272.76 permitem que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam um ServiceWorkerContextWrapper::Chamada DeleteAndStartOver, relacionada às funções NotifyStartedCaching e NotifyFinishedCaching.
CVE-2015-1220	A vulnerabilidade use-after-free no Blink, como usada no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado ao alavancar o ordenamento incorreto de operações no encadeamento Web SQL Database relativo ao principal thread, relacionado à função de desligamento em web / WebKit.cpp.
CVE-2015-1220	A vulnerabilidade use-after-free na função GIFImageReader::parseData em platform / image-decoders / gif / GIFImageReader.cpp no Blink, como usada no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço ou possivelmente Outro impacto não especificado por meio de um tamanho de quadro criado em uma imagem GIF.
CVE-2015-1219	O estouro de inteiro na função SkMallocPixelRef::NewAllocate no core / SkMallocPixelRef.cpp no Skia, como usado no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores que acionam uma tentativa de alocação de uma grande quantidade de memória durante a renderização do WebGL.
CVE-2015-1218	Várias vulnerabilidades de uso após livre na implementação do DOM no Blink, usadas no Google Chrome antes de 41.0.2272.76, permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam o movimento de um elemento SCRIPT para diferentes documentos, relacionados a (1) a função HTMLScriptElement::didMoveToNewDocument em core / html / HTMLScriptElement.cpp e (2) a função SVGScriptElement::didMoveToNewDocument em core / svg / SVGScriptElement.cpp.
CVE-2015-1217	A função V8LazyEventListener::prepareListenerObject em bindings / core / v8 / V8LazyEventListener.cpp nas ligações V8 no Blink, conforme usada no Google Chrome antes de 41.0.2272.76, não compila os listeners corretamente, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto através de vetores que alavancam "tipo de confusão".
CVE-2015-1216	A vulnerabilidade use-after-free na função V8Window::namedPropertyGetterCustom em bindings / core / v8 / custom / V8WindowCustom.cpp nas vinculações V8 no Blink, conforme usada no Google Chrome antes de 41.0.2272.76, permite que

Nome	Descrição
	atacantes remotos causem a negação de serviço ou possivelmente não especificou outro impacto através de vetores que acionam um destaque de quadros.
CVE-2015-1215	A implementação de filtros no Skia, como usada no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam uma operação de gravação fora dos limites.
CVE-2015-1214	O estouro de inteiro na implementação do SkAutoSTArray em include / core / SkTemplates.h na implementação de filtros no Skia, como usado no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores que acionam uma ação de reconfiguração com um grande valor de contagem, levando a uma operação de gravação fora dos limites.
CVE-2015-1213	A função SkBitmap :: ReadRawPixels no core / SkBitmap.cpp na implementação de filtros no Skia, como usada no Google Chrome antes de 41.0.2272.76, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores que acionam uma saída -of-bounds operação de gravação.
CVE-2015-1212	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 40.0.2214.111 no Windows, OS X e Linux e antes de 40.0.2214.109 no Android permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2015-1211	A função OriginCanAccessServiceWorkers no conteúdo / browser / service_worker / service_worker_dispatcher_host.cc no Google Chrome antes de 40.0.2214.111 no Windows, OS X e Linux e antes de 40.0.2214.109 no Android não restringe adequadamente o esquema de URI durante um registro do ServiceWorker, o que permite acesso remoto invasores para obter privilégios através de um sistema de arquivos: URI.
CVE-2015-1210	A função V8ThrowException :: createDOMException em ligações / core / v8 / V8ThrowException.cpp nas ligações da V8 no Blink, como usada no Google Chrome antes de 40.0.2214.111 no Windows, OS X e Linux e antes de 40.0.2214.109 no Android, não Considere adequadamente as restrições de acesso a quadros durante o lançamento de uma exceção, o que permite que invasores remotos ignorem a Política de mesma origem por meio de um site criado.
CVE-2015-1209	Vulnerabilidade usar-depois-livre na função VisibleSelection :: nonBoundaryShadowTreeRootNode no core / editing / VisibleSelection.cpp na implementação do DOM no Blink, conforme usado no Google Chrome antes de 40.0.2214.111 no Windows, OS X e Linux e antes de 40.0.2214.109 no Android, permite que atacantes remotos causem uma negação de serviço ou

Nome	Descrição
	possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que aciona o manuseio inadequado de uma âncora de raiz de sombra.
CVE-2015-1207	A vulnerabilidade do Double-free em libavformat / mov.c no FFMPEG no Google Chrome 41.0.2251.0 permite que atacantes remotos causem uma negação de serviço (corrupção de memória e falha) por meio de um arquivo .m4a criado.
CVE-2015-1206	O estouro de buffer baseado em heap no Google Chrome antes do M40 permite que atacantes remotos causem uma negação de serviço (gravação de memória não paginada e falha de processo) por meio de um arquivo MP4 criado.
CVE-2015-1205	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 40.0.2214.91 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-9689	content / renderer / device_sensors / device_orientation_event_pump.cc no Google Chrome anterior a 41.0.2272.76 não restringe adequadamente o acesso a dados de giroscópio de alta taxa, o que facilita para invasores remotos obter sinais de fala do ambiente físico de um dispositivo por meio de um site criado ouve eventos de orientação de destino, uma vulnerabilidade diferente da CVE-2015-1231.
CVE-2014-9654	O pacote Expressões regulares em Componentes internacionais para Unicode (ICU) para C / C ++ antes de 2014-12-03, conforme usado no Google Chrome antes de 40.0.2214.91, calcula determinados valores sem garantir que eles possam ser representados em um campo de 24 bits, que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de uma string criada, um problema relacionado ao CVE-2014-7923.
CVE-2014-9648	components / navigation_interception / intercept_navigation_resource_throttle.cc no Google Chrome antes de 40.0.2214.91 no Android não restringe adequadamente o uso da intenção: URLs para abrir um aplicativo após a navegação em um site, o que permite que invasores remotos causem uma negação de serviço (perda de navegador acesso a esse site) por meio de código JavaScript criado, conforme demonstrado pelo pandora.com e pelo aplicativo Pandora, uma vulnerabilidade diferente da CVE-2015-1205.
CVE-2014-9647	A vulnerabilidade "usar-depois-livre" no PDFium, usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento PDF criado, relacionado a fpdfsdk / src / fpdfview.cpp e fpdfsdk / src / fsdk_mgr.cpp, uma vulnerabilidade diferente da CVE-2015-1205.
CVE-2014-9646	A vulnerabilidade do caminho de pesquisa do Windows não mapeado na função GoogleChromeDistribution ::

Nome	Descrição
CVE-2014-7967	DoPostUninstallOperations no installer / util / google_chrome_distribution.cc no recurso de pesquisa de desinstalação do Google Chrome antes de 40.0.2214.91 permite que os usuários locais obtenham privilégios por meio de um programa de cavalo de Tróia no diretório% SYSTEMDRIVE% , conforme demonstrado pelo program.exe, uma vulnerabilidade diferente da CVE-2015-1205.
CVE-2014-7948	Várias vulnerabilidades não especificadas no Google V8 anteriores a 3.28.71.15, conforme usadas no Google Chrome antes de 38.0.2125.101, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-7947	A função AppCacheUpdateJob :: URLFetcher :: OnResponseStarted em content / browser / appcache / appcache_update_job.cc no Google Chrome antes de 40.0.2214.91 continua com o armazenamento em cache do AppCache para sessões SSL, mesmo se houver um erro de certificado X.509, que permite invasores intermediários para falsificar o conteúdo do aplicativo HTML5 por meio de um certificado criado.
CVE-2014-7946	O OpenJPEG antes de r2944, usado no PDFium no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento PDF criado, relacionado a j2k.c, jp2.c, pi .c, t1.c, t2.c e tcd.c.
CVE-2014-7945	A função RenderTable :: simplifiedNormalFlowLayout em core / rendering / RenderTable.cpp no Blink, como usada no Google Chrome antes de 40.0.2214.91, pula legendas durante o layout da tabela em certas situações, o que permite que atacantes remotos causem uma negação de serviço (fora de -bounds read) através de vetores não especificados relacionados à implementação de fontes.
CVE-2014-7944	O OpenJPEG anterior ao r2908, usado no PDFium no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento PDF criado, relacionado a j2k.c, jp2.c e t2.c.
CVE-2014-7943	A função sycc422_to_rgb em fxcodec / codec / fx_codec_jpx_opj.cpp no PDFium, como usada no Google Chrome antes de 40.0.2214.91, não manipula corretamente valores ímpares de largura da imagem, o que permite que atacantes remotos causem uma negação de serviço (fora dos limites ler) através de um documento PDF criado.
CVE-2014-7942	O Skia, como usado no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.

Nome	Descrição
CVE-2014-7941	especificado por meio de vetores desconhecidos.
CVE-2014-7940	A função SelectionOwner :: ProcessTarget em ui / base / x / selection_owner.cc na implementação da interface do usuário no Google Chrome anterior a 40.0.2214.91 usa um tipo de dados incorreto para um determinado valor de tamanho, o que permite que atacantes remotos causem uma negação de serviço -of-bounds) através de dados X11 criados.
CVE-2014-7940	A implementação do classificador em i18n / ucol.cpp em Componentes Internacionais para Unicode (ICU) 52 através da revisão SVN 293126, usada no Google Chrome antes de 40.0.2214.91, não inicializa memória para uma estrutura de dados, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente não ter especificado outro impacto por meio de uma sequência de caracteres criada.
CVE-2014-7939	O Google Chrome antes de 40.0.2214.91, quando o proxy Harmony no Google V8 está ativado, permite que atacantes remotos contornem a Política de mesma origem por meio de código JavaScript criado com chamadas Proxy.create e console.log, relacionadas a respostas HTTP sem "X" Content-Type-Options: nosniff "cabeçalho.
CVE-2014-7938	A implementação de Fontes no Google Chrome anterior a 40.0.2214.91 permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2014-7937	Múltiplos erros off-one no libavcodec / vorbisdec.c no FFmpeg antes do 2.4.2, como usado no Google Chrome antes de 40.0.2214.91, permitem que atacantes remotos causem uma negação de serviço (use-após-free) ou possivelmente não tenham especificado outro impacto através de dados Vorbis I criados.
CVE-2014-7936	A vulnerabilidade "usar-depois-livre" na função ZoomBubbleView :: Close no navegador / ui / views / location_bar / zoom_bubble_view.cc na implementação do Views no Google Chrome antes de 40.0.2214.91 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outros não especificados impacto através de um documento elaborado que aciona a manutenção inadequada de uma bolha de zoom.
CVE-2014-7935	A vulnerabilidade "usar-depois-livre" no navegador / fala / tts_message_filter.cc na implementação de fala no Google Chrome antes de 40.0.2214.91 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo declarações de uma guia fechada.
CVE-2014-7934	A vulnerabilidade "usar-depois-livre" na implementação do DOM no Blink, usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados à ausência inesperada de estruturas de dados do documento.

Nome	Descrição
CVE-2014-7933	A vulnerabilidade use-after-free na função matroska_read_seek em libavformat / matroskademux.c no FFmpeg antes de 2.5.1, como usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um arquivo Matroska criado que aciona a manutenção inadequada dos dados das faixas.
CVE-2014-7932	A vulnerabilidade Use-after-free na função Element :: detach no core / dom / Element.cpp na implementação do DOM no Blink, como usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou possivelmente Outro impacto não especificado via vetores envolvendo atualizações pendentes de elementos destacados.
CVE-2014-7931	O factory.cc no Google V8, usado no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que aciona a manutenção inadequada dos indicadores da loja de suporte.
CVE-2014-7930	A vulnerabilidade use-after-free no core / events / TreeScopeEventContext.cpp na implementação do DOM no Blink, usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que aciona a manutenção inadequada dos dados do TreeScope.
CVE-2014-7929	A vulnerabilidade "use-after-free" na função HTMLScriptElement :: didMoveToNewDocument no core / html / HTMLScriptElement.cpp na implementação do DOM no Blink, como usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou possivelmente Outro impacto não especificado via vetores que envolvem o movimento de um elemento SCRIPT em todos os documentos.
CVE-2014-7928	O hydrogen.cc no Google V8, como usado no Google Chrome antes de 40.0.2214.91, não manipula corretamente arrays com buracos, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado uma cópia de matriz.
CVE-2014-7927	A função SimplifiedLowering :: DoLoadBuffer no compilador / simplified-lowering.cc no Google V8, usada no Google Chrome antes de 40.0.2214.91, não escolhe adequadamente um tipo de dados inteiro, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente não especificou outro impacto através do código JavaScript criado.
CVE-2014-7926	O pacote Expressões Regulares no International Components for Unicode (ICU) 52 antes da revisão SVN 292944, usado no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos

Nome	Descrição
	causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados para um quantificador de comprimento zero.
CVE-2014-7925	A vulnerabilidade "usar-depois-livre" na implementação do WebAudio no Blink, usada no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores que acionam um encadeamento de renderização de áudio no qual AudioNode os dados são mantidos incorretamente.
CVE-2014-7924	A vulnerabilidade "usar-depois-livre" na implementação do IndexedDB no Google Chrome antes de 40.0.2214.91 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado acionando referências BLOB duplicadas, relacionadas a conteúdo / browser / indexed_db / indexed_db_callbacks.cc e content / browser / indexed_db / indexed_db_dispatcher_host.cc.
CVE-2014-7923	O pacote Expressões Regulares no International Components for Unicode (ICU) 52 antes da revisão SVN 292944, usado no Google Chrome antes de 40.0.2214.91, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados para uma expressão de olhar para trás.
CVE-2014-7910	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 39.0.2171.65 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-7909	effects / SkDashPathEffect.cpp no Skia, como usado no Google Chrome antes de 39.0.2171.65, calcula uma chave de hash usando valores inteiros não inicializados, o que pode permitir que atacantes remotos causem uma negação de serviço ao renderizar dados criados.
CVE-2014-7908	Vários overflows inteiros na função CheckMov em media / base / container_names.cc no Google Chrome antes de 39.0.2171.65 permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um átomo grande em (1) MPEG-4 ou (2) dados QuickTime .mov.
CVE-2014-7907	Várias vulnerabilidades de uso após livre em modules / screen_orientation / ScreenOrientationController.cpp no Blink, como usadas no Google Chrome antes de 39.0.2171.65, permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam o tratamento inadequado um quadro desanexado, relacionado aos métodos (1) lock e (2) unlock.
CVE-2014-7906	A vulnerabilidade "usar-depois-livre" nos plug-in do Google Chrome antes do 39.0.2171.65 permite que invasores remotos causem

Nome	Descrição
	uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de conteúdo Flash criado que aciona uma tentativa de acesso ao PepperMediaDeviceManager fora do tempo de vida do objeto.
CVE-2014-7905	O Google Chrome anterior ao 39.0.2171.65 no Android não impede a navegação para um URL nos casos em que a intenção do URL não é igual a CATEGORY_BROWSABLE, o que permite que atacantes remotos contornem as restrições de acesso pretendidas por meio de um site criado.
CVE-2014-7904	O estouro de buffer no Skia, como usado no Google Chrome antes de 39.0.2171.65, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2014-7903	O estouro de buffer no OpenJPEG antes de r2911 no PDFium, como usado no Google Chrome antes de 39.0.2171.65, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de uma imagem JPEG criada.
CVE-2014-7902	A vulnerabilidade "usar-depois-de-graça" no PDFium, usada no Google Chrome antes de 39.0.2171.65, permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento PDF criado.
CVE-2014-7901	O estouro de inteiro na função opj_t2_read_packet_data em fxcodec / fx_libopenjpeg / libopenjpeg20 / t2.c no OpenJPEG no PDFium, como usado no Google Chrome antes de 39.0.2171.65, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um longo segmento em uma imagem JPEG.
CVE-2014-7900	A vulnerabilidade use-after-free na função CPDF_Parser :: IsLinearizedFile em fpdfapi / fpdf_parser / fpdf_parser_parser.cpp no PDFium, como usada no Google Chrome antes de 39.0.2171.65, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via um documento PDF criado.
CVE-2014-7899	O Google Chrome, anterior a 38.0.2125.101, permite que atacantes remotos falsifiquem a barra de endereço, colocando uma substrobobob: substring no início do URL, seguida pelo esquema de URI original e por uma string de nome de usuário longa.
CVE-2014-3803	O recurso SpeechInput no Blink, usado no Google Chrome antes de 35.0.1916.114, permite que atacantes remotos habilitem o acesso ao microfone e obtenham texto de reconhecimento de fala sem indicação por meio de um elemento INPUT com um atributo -webkit-speech.
CVE-2014-3201	core / rendering / compositing / RenderLayerCompositor.cpp no Blink, como usado no Google Chrome antes de 38.0.2125.102 no Android, não manipula adequadamente uma determinada condição

Nome	Descrição
	de estouro do IFRAME, que permite que atacantes remotos falsifiquem conteúdo por meio de um site criado que interfira com o Barra de rolagem.
CVE-2014-3200	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 38.0.2125.101 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-3199	A função wrap em bindings / core / v8 / custom / V8EventCustom.cpp nas vinculações V8 no Blink, conforme usado no Google Chrome antes de 38.0.2125.101, tem um resultado de fallback incorreto para falhas de seleção de wrapper, o que permite que atacantes remotos causem uma falha negação de serviço por meio de vetores que acionam a interrupção de um processo de trabalho que estava manipulando um objeto Event.
CVE-2014-3198	A função Instance :: HandleInputEvent em pdf / instance.cc no componente PDFium no Google Chrome antes de 38.0.2125.101 interpreta um determinado valor -1 como um índice em vez de um código de erro sem página visível, que permite que atacantes remotos causem negação de serviço (leitura fora dos limites) através de vetores não especificados.
CVE-2014-3197	A função NavigationScheduler :: schedulePageBlock no core / loader / NavigationScheduler.cpp no Blink, como usada no Google Chrome antes de 38.0.2125.101, não fornece dados substitutos para páginas bloqueadas pelo auditor do XSS, o que permite que atacantes remotos obtenham informações confidenciais por meio de um site criado.
CVE-2014-3196	base / memory / shared_memory_win.cc no Google Chrome antes de 38.0.2125.101 no Windows não implementa adequadamente restrições somente leitura na memória compartilhada, o que permite que invasores ignorem um mecanismo de proteção de caixa de proteção por meio de vetores não especificados.
CVE-2014-3195	O Google V8, usado no Google Chrome antes de 38.0.2125.101, não controla adequadamente as alocações de memória heap do JavaScript como alocações de memória não inicializada e não concatena corretamente matrizes de números de ponto flutuante de precisão dupla, o que permite que atacantes remotos obtenham informações confidenciais via código JavaScript criado, relacionado às funções PagedSpace :: AllocateRaw e NewSpace :: AllocateRaw em heap / spaces-inl.h, a função LargeObjectSpace :: AllocateRaw em heap / spaces.cc e a função Runtime_ArrayConcat em runtime.cc.
CVE-2014-3194	A vulnerabilidade "usar-depois-livre" na implementação do Web Workers no Google Chrome antes de 38.0.2125.101 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2014-3193	A função SessionService :: GetLastSession em browser / sessions /

Nome	Descrição
CVE-2014-3192	session_service.cc no Google Chrome antes de 38.0.2125.101 permite que atacantes remotos causem uma negação de serviço (use-após-livre) ou possivelmente tenham outro impacto não especificado através de vetores que alavancam "tipo confusão "para processamento de retorno de chamada.
CVE-2014-3191	A vulnerabilidade use-after-free na função ProcessingInstruction :: setXSLStyleSheet no core / dom / ProcessingInstruction.cpp na implementação DOM no Blink, como usada no Google Chrome antes de 38.0.2125.101, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham Outro impacto não especificado através de vetores desconhecidos.
CVE-2014-3190	A vulnerabilidade de uso após a liberação no Blink, usada no Google Chrome antes de 38.0.2125.101, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que acione uma atualização de posição de widget que interaja incorretamente com o render tree, relacionado à função FrameView :: updateLayoutAndStyleForPainting em core / frame / FrameView.cpp e a função RenderLayerScrollableArea :: setScrollOffset em core / rendering / RenderLayerScrollableArea.cpp.
CVE-2014-3189	A vulnerabilidade use-after-free na função Event :: currentTarget no core / events / Event.cpp no Blink, como usada no Google Chrome antes de 38.0.2125.101, permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente Outro impacto não especificado via código JavaScript criado que acessa a propriedade de caminho de um objeto Event.
CVE-2014-3188	A função chrome_pdf :: CopyImage em pdf / draw_utils.cc no componente PDFium no Google Chrome antes de 38.0.2125.101 não valida corretamente dimensões de dados de imagem, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) ou possivelmente não especificou outro impacto através de vetores desconhecidos.
CVE-2014-3188	O Google Chrome anterior a 38.0.2125.101 e o Chrome OS anteriores a 38.0.2125.101 não lidam adequadamente com a interação do IPC e do Google V8, que permite que atacantes remotos executem código arbitrário por meio de vetores envolvendo dados JSON, relacionados à análise imprópria de um índice de escape por ParseJsonObject no json-parser.h.
CVE-2014-3187	O Google Chrome anterior a 37.0.2062.60 e 38.x antes de 38.0.2125.59 no iOS não restringe adequadamente o processamento de (1) facetime: // e (2) facetime-audio: // URLs, o que permite que atacantes remotos obtenham vídeo e áudio dados de um dispositivo através de um site criado.
CVE-2014-3179	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 37.0.2062.120 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto

Nome	Descrição
	por meio de vetores desconhecidos.
CVE-2014-3178	A vulnerabilidade use-after-free no core / dom / Node.cpp no Blink, usada no Google Chrome antes de 37.0.2062.120, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando o tratamento inadequado da árvore de renderização inconsistências.
CVE-2014-3177	O Google Chrome anterior a 37.0.2062.94 não lida corretamente com a interação de extensões, IPC, a API de sincronização e o Google V8, que permite que atacantes remotos executem código arbitrário por meio de vetores não especificados, uma vulnerabilidade diferente da CVE-2014-3176.
CVE-2014-3176	O Google Chrome anterior a 37.0.2062.94 não lida adequadamente com a interação de extensões, IPC, a API de sincronização e o Google V8, que permite que atacantes remotos executem código arbitrário por meio de vetores não especificados, uma vulnerabilidade diferente da CVE-2014-3177.
CVE-2014-3175	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 37.0.2062.94 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos, relacionados à função load_truetype_glyph no truetype / ttgload.c no FreeType e em outras funções em outros componentes.
CVE-2014-3174	modules / webaudio / BiquadDSPKernel.cpp na implementação da Web Audio API no Blink, como usado no Google Chrome antes de 37.0.2062.94, não considera propriamente os threads simultâneos durante as tentativas de atualizar os coeficientes do filtro biquad, que permite que atacantes remotos causem uma negação de serviço (leitura de memória não inicializada) por meio de chamadas de API criadas.
CVE-2014-3173	A implementação do WebGL no Google Chrome anterior a 37.0.2062.94 não garante que chamadas claras interajam corretamente com o estado de um buffer de desenho, o que permite que atacantes remotos causem uma negação de serviço (leitura de memória não inicializada) por meio de um elemento CANVAS elaborado, relacionado a gpu / command_buffer / service / framebuffer_manager.cc e gpu / command_buffer / service / gles2_cmd_decoder.cc.
CVE-2014-3172	A API de extensão do depurador no navegador / extensions / api / debugger / debugger_api.cc no Google Chrome anterior a 37.0.2062.94 não valida o URL de um separador antes de uma operação de anexação, o que permite que atacantes remotos contornem as limitações de acesso pretendidas através de uma extensão URL, conforme demonstrado por um URL chrome: //.
CVE-2014-3171	A vulnerabilidade use-after-free nas ligações V8 no Blink, conforme usada no Google Chrome antes de 37.0.2062.94, permite que atacantes remotos causem uma negação de serviço ou

Nome	Descrição
	possivelmente tenham outro impacto não especificado aproveitando o uso indevido de operações de adição HashMap em vez do conjunto HashMap operações, relacionadas a ligações / core / v8 / DOMWrapperMap.h e ligações / core / v8 / SerializedScriptValue.cpp.
CVE-2014-3170	extensions / common / url_pattern.cc no Google Chrome anterior a 37.0.2062.94 não impede o uso de um caractere '\0' em um nome de host, o que permite que atacantes remotos falsifiquem o diálogo de permissão de extensão confiando no truncamento após esse caractere.
CVE-2014-3169	A vulnerabilidade use-after-free no core / dom / ContainerNode.cpp na implementação do DOM no Blink, usada no Google Chrome antes de 37.0.2062.94, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando a execução de scripts que ocorre antes da notificação de remoção do nó.
CVE-2014-3168	A vulnerabilidade "usar-depois-livre" na implementação do SVG no Blink, usada no Google Chrome antes de 37.0.2062.94, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando o cache incorreto associado à animação.
CVE-2014-3167	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 36.0.1985.143 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-3166	A implementação da PKP (Public Key Pinning) no Google Chrome antes de 36.0.1985.143 no Windows, OS X e Linux e antes de 36.0.1985.135 no Android não considera corretamente as propriedades das conexões SPDY, o que permite que atacantes remotos obtenham informações confidenciais aproveitando o uso de vários nomes de domínio.
CVE-2014-3165	A vulnerabilidade use-after-free em modules / websockets / WorkerThreadableWebSocketChannel.cpp na implementação do Web Sockets no Blink, usada no Google Chrome antes de 36.0.1985.143, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores que disparar uma vida útil inesperadamente longa de um objeto temporário durante a conclusão do método.
CVE-2014-3162	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 36.0.1985.125 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-3161	A função WebMediaPlayerAndroid :: load em content / renderer / media / android / webmediaplayer_android.cc no Google Chrome antes de 36.0.1985.122 no Android não interage adequadamente com redirecionamentos, o que permite que atacantes remotos

Nome	Descrição
	contornem a Política de mesma origem por meio de um site criado hospeda um fluxo de vídeo.
CVE-2014-3160	A função ResourceFetcher :: canRequest no core / fetch / ResourceFetcher.cpp no Blink, como usada no Google Chrome antes de 36.0.1985.125, não restringe adequadamente as solicitações de sub-recursos associados aos arquivos SVG, o que permite que atacantes remotos contornem a Política de mesma origem por meio de arquivo trabalhado.
CVE-2014-3159	A função WebContentsDelegateAndroid :: OpenURLFromTab em componentes / web_contents_delegate_android / web_contents_delegate_android.cc no Google Chrome anterior a 36.0.1985.122 no Android não restringe adequadamente o carregamento de URL, o que permite que invasores remotos falsifiquem o URL na omnibox por meio de vetores não especificados.
CVE-2014-3157	O estouro de buffer com base em heap na função FFmpegVideoDecoder :: GetVideoBuffer em media / filters / ffmpeg_video_decoder.cc no Google Chrome antes de 35.0.1916.153 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando estruturas de dados VideoFrame que também são pequeno para interação adequada com uma biblioteca FFmpeg subjacente.
CVE-2014-3156	O estouro de buffer na implementação da área de transferência no Google Chrome anterior a 35.0.1916.153 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam dados de bitmap inesperados, relacionados a conteúdo / renderizador / renderer_clipboard_client.cc e conteúdo / renderizador / webclipboard_impl.cc.
CVE-2014-3155	net / spdy / spdy_write_queue.cc na implementação do SPDY no Google Chrome antes de 35.0.1916.153 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) aproveitando a manutenção incorreta da fila.
CVE-2014-3154	A vulnerabilidade usar-depois-livre na função ChildThread :: Shutdown em content / child / child_thread.cc na API do sistema de arquivos no Google Chrome antes de 35.0.1916.153 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados para um desligamento de Blink.
CVE-2014-3152	O underflow inteiro na função LCodeGen :: PrepareKeyedOperand em arm / lithium-codegen-arm.cc no Google V8 anterior a 3.25.28.16, conforme usado no Google Chrome antes de 35.0.1916.114, permite que atacantes remotos causem uma negação de serviço ou possivelmente não tenham especificado outro impacto através de vetores que acionam um valor de chave negativo.

Nome	Descrição
CVE-2014-1749	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 35.0.1916.114 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-1748	A função ScrollView :: paint na plataforma / scroll / ScrollView.cpp no Blink, como usada no Google Chrome antes de 35.0.1916.114, permite que atacantes remotos falsifiquem a interface do usuário estendendo a pintura da barra de rolagem para o quadro principal.
CVE-2014-1747	A vulnerabilidade de cross-site scripting (XSS) na função DocumentLoader :: maybeCreateArchive no core / loader / DocumentLoader.cpp no Blink, usada no Google Chrome antes de 35.0.1916.114, permite que atacantes remotos injetem scripts da Web ou HTML arbitrários por meio do conteúdo MHTML criado , também conhecido como "Universal XSS (UXSS)".
CVE-2014-1746	A função InMemoryUrlProtocol :: Read em media / filters / in_memory_url_protocol.cc no Google Chrome anterior a 35.0.1916.114 depende de um tipo de dados inteiro insuficientemente grande, que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores que acionam o uso de um buffer grande.
CVE-2014-1745	A vulnerabilidade de uso após a liberação na implementação de SVG no Blink, usada no Google Chrome antes de 35.0.1916.114, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores que acionam a remoção de um objeto SVGFontFaceElement relacionado a core / svg / SVGFontFaceElement.cpp.
CVE-2014-1744	O estouro de número inteiro na função AudioInputRendererHost :: OnCreateStream no conteúdo / browser / renderer_host / media / audio_input_renderer_host.cc no Google Chrome antes de 35.0.1916.114 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam um grande compartilhamento - alocação de memória.
CVE-2014-1743	A vulnerabilidade use-after-free na função StyleElement :: removedFromDocument no core / dom / StyleElement.cpp no Blink, como usada no Google Chrome antes de 35.0.1916.114, permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham Outro impacto não especificado através do código JavaScript criado que aciona a mutação de árvore.
CVE-2014-1742	A vulnerabilidade use-after-free na função FrameSelection :: updateAppearance em core / editing / FrameSelection.cpp no Blink, como usada no Google Chrome antes de 34.0.1847.137, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado aproveitando a manipulação indevida do RenderObject.

Nome	Descrição
CVE-2014-1741	Vários transbordamentos de números inteiros na funcionalidade de substituição de dados na implementação da interface CharacterData no core / dom / CharacterData.cpp no Blink, conforme usado no Google Chrome antes de 34.0.1847.137, permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores relacionados a intervalos.
CVE-2014-1740	Várias vulnerabilidades de uso livre em net / websockets / websocket_job.cc na implementação de WebSockets no Google Chrome anteriores a 34.0.1847.137 permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à exclusão de WebSocketJob.
CVE-2014-1736	O estouro de número inteiro no api.cc no Google V8, usado no Google Chrome antes de 34.0.1847.131 no Windows e OS X e antes de 34.0.1847.132 no Linux, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um grande valor do comprimento.
CVE-2014-1735	Várias vulnerabilidades não especificadas no Google V8 anteriores a 3.24.35.33, conforme usadas no Google Chrome antes de 34.0.1847.131 no Windows e OS X e antes de 34.0.1847.132 no Linux, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-1734	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 34.0.1847.131 no Windows e OS X e anteriores a 34.0.1847.132 no Linux permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-1733	A função PointerCompare em codegen.cc no Seccomp-BPF, como usada no Google Chrome antes de 34.0.1847.131 no Windows e OS X e antes de 34.0.1847.132 no Linux, não mescla blocos corretamente, o que pode permitir que atacantes remotos contornem restrições de sandbox pretendidas alavancando o acesso renderizador.
CVE-2014-1732	A vulnerabilidade de uso depois de livre no navegador / ui / views / speech_recognition_bubble_views.cc no Google Chrome antes de 34.0.1847.131 no Windows e OS X e antes de 34.0.1847.132 no Linux permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via um elemento INPUT que aciona a presença de uma janela Speech Recognition Bubble por uma duração incorreta.
CVE-2014-1731	core / html / HTMLSelectElement.cpp na implementação do DOM no Blink, conforme usado no Google Chrome antes de 34.0.1847.131 no Windows e OS X e antes do 34.0.1847.132 no Linux, não verifica adequadamente o estado do renderizador em um evento de foco, o que permite acesso remoto invasores

Nome	Descrição
	causarem uma negação de serviço ou possivelmente não especificaram outro impacto por meio de vetores que aproveitam a "confusão de tipo" para elementos SELECT.
CVE-2014-1730	O Google V8, usado no Google Chrome antes de 34.0.1847.131 no Windows e OS X e antes de 34.0.1847.132 no Linux, não armazena metadados de internacionalização corretamente, o que permite que atacantes remotos contornem as restrições de acesso pretendidas aproveitando a "confusão de tipos" e a propriedade de leitura valores, relacionados a i18n.js e runtime.cc.
CVE-2014-1729	Várias vulnerabilidades não especificadas no Google V8 anteriores a 3.24.35.22, conforme usadas no Google Chrome antes de 34.0.1847.116, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-1728	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 34.0.1847.116 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2014-1727	A vulnerabilidade "usar-depois-de-graça" no conteúdo / renderizador / renderer_webcolorchooser_impl.h no Google Chrome antes de 34.0.1847.116 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a formulários.
CVE-2014-1726	A implementação de arrastar no Google Chrome antes de 34.0.1847.116 permite que invasores remotos assistidos por usuário ignorem a Política de mesma origem e forjam nomes de caminho locais, aproveitando o acesso do renderizador.
CVE-2014-1725	A função base64DecodeInternal em wtf / text / Base64.cpp no Blink, como usada no Google Chrome antes de 34.0.1847.116, não manipula adequadamente dados de strings compostos exclusivamente de caracteres em branco, o que permite que atacantes remotos causem uma negação de serviço (fora de - bounds ler) através de uma chamada de método window.atob.
CVE-2014-1724	A vulnerabilidade "usar-depois-de-graça" no Free (b) Soft Laboratory Dispatcher 0.7.1, usado no Google Chrome antes de 34.0.1847.116, permite que atacantes remotos causem uma negação de serviço (interrupção do aplicativo) ou possivelmente tenham outro impacto não especificado através de um solicitação de texto para fala.
CVE-2014-1723	A função UnescapeURLWithOffsetsImpl em net / base / escape.cc no Google Chrome anterior a 34.0.1847.116 não lida corretamente com identificadores de recursos internacionalizados (IRIs) bidirecionais, o que facilita para invasores remotos falsificar URLs por meio do uso da direita para a esquerda (RTL) texto Unicode.
CVE-2014-1722	A vulnerabilidade Use-after-free na função RenderBlock :: addChildIgnoringAnonymousColumnBlocks no core / rendering /

Nome	Descrição
CVE-2014-1721	RenderBlock.cpp no Blink, como usado no Google Chrome antes de 34.0.1847.116, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores envolvendo a adição de um nó filho.
CVE-2014-1720	O Google V8, usado no Google Chrome antes de 34.0.1847.116, não implementa corretamente a desativação lenta, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente não tenham outro impacto por código JavaScript criado, conforme demonstrado pelo manuseio inadequado de uma alocação de heap de um número fora do intervalo Small Integer (aka smi).
CVE-2014-1720	A vulnerabilidade "usar-depois-livre" na função HTMLBodyElement :: insertedInto no core / html / HTMLBodyElement.cpp no Blink, conforme usada no Google Chrome antes de 34.0.1847.116, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores envolvendo atributos.
CVE-2014-1719	A vulnerabilidade use-after-free na função WebSharedWorkerStub :: OnTerminateWorkerContext em content / worker / websharedworker_stub.cc na implementação de Web Workers no Google Chrome antes de 34.0.1847.116 permite que atacantes remotos causem uma negação de serviço (corrupção de memória de heap) ou possivelmente Outro impacto não especificado por meio de vetores que acionam uma terminação do SharedWorker durante o carregamento do script.
CVE-2014-1718	O estouro de inteiro na função SoftwareFrameManager :: SwapToNewFrame em content / browser / renderer_host / software_frame_manager.cc no compositor de software no Google Chrome antes de 34.0.1847.116 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam um tentativa de mapeamento de uma grande quantidade de memória renderizador.
CVE-2014-1717	O Google V8, usado no Google Chrome antes de 34.0.1847.116, não usa corretamente conversões numéricas durante o tratamento de matrizes digitadas, o que permite que invasores remotos causem uma negação de serviço (acesso a matriz fora do limite) ou possivelmente outro impacto não especificado via código JavaScript criado.
CVE-2014-1716	A vulnerabilidade de script entre sites (XSS) na função Runtime_SetPrototype em runtime.cc no Google V8, usada no Google Chrome antes de 34.0.1847.116, permite que invasores remotos injetem scripts da Web ou HTML arbitrários por meio de vetores não especificados, também conhecidos como "XSS universal (UXSS)) "
CVE-2014-1715	A vulnerabilidade de travessia de diretório no Google Chrome anterior a 33.0.1750.152 no OS X e no Linux e antes de 33.0.1750.154 no Windows tem vetores de impacto e de ataque

Nome	Descrição
	não especificados.
CVE-2014-1714	A função ScopedClipboardWriter :: WritePickledData em ui / base / clipboard / scoped_clipboard_writer.cc no Google Chrome anterior a 33.0.1750.152 no OS X e Linux e antes de 33.0.1750.154 no Windows não verifica um determinado valor de formato, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente ter outro impacto não especificado através de vetores relacionados à área de transferência.
CVE-2014-1713	A vulnerabilidade use-after-free na função AttributeSetter em bindings / templates / attributes.cpp nas ligações no Blink, conforme usada no Google Chrome antes de 33.0.1750.152 no OS X e Linux e antes de 33.0.1750.154 no Windows, permite que atacantes remotos causar uma negação de serviço ou possivelmente ter outro impacto não especificado via vetores envolvendo o valor document.location.
CVE-2014-1711	O driver da GPU no kernel no Google Chrome OS anterior a 33.0.1750.152 permite que atacantes remotos causem uma negação de serviço (gravação fora do limite) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2014-1710	A função AsyncPixelTransfersCompletedQuery :: End em gpu / command_buffer / service / query_manager.cc no Google Chrome, conforme usada no Google Chrome OS anterior a 33.0.1750.152, não verifica se uma determinada posição está dentro dos limites de um segmento de memória compartilhada, que permite que invasores remotos causem uma negação de serviço (corrupção da memória do buffer de comando da GPU) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2014-1708	A implementação de inicialização no Google Chrome OS anterior a 33.0.1750.152 não considera adequadamente a persistência de arquivos, o que permite que atacantes remotos executem código arbitrário por meio de vetores não especificados.
CVE-2014-1707	A vulnerabilidade de travers de diretório em CrosDisks no Google Chrome OS anterior a 33.0.1750.152 não possui vetores de impacto e de ataque.
CVE-2014-1706	crosh no Google Chrome OS antes de 33.0.1750.152 permite que os atacantes injetem comandos através de vetores não especificados.
CVE-2014-1705	O Google V8, usado no Google Chrome antes de 33.0.1750.152 no OS X e Linux e antes de 33.0.1750.154 no Windows, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2014-1704	Várias vulnerabilidades não especificadas no Google V8 anteriores a 23.03.17.18, conforme usadas no Google Chrome antes de 33.07.17.149, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de

Nome	Descrição
vetores desconhecidos.	
CVE-2014-1703	A vulnerabilidade use-after-free na função WebSocketDispatcherHost :: SendOrDrop em content / browser / renderer_host / websocket_dispatcher_host.cc na implementação do Web Sockets no Google Chrome antes de 33.0.1750.149 pode permitir que atacantes remotos ignorem o mecanismo de proteção do sandbox, aproveitando uma exclusão incorreta em um determinado caso de falha.
CVE-2014-1702	A vulnerabilidade use-after-free na função DatabaseThread :: cleanupDatabaseThread em modules / webdatabase / DatabaseThread.cpp na implementação do banco de dados da web no Blink, usada no Google Chrome antes de 33.0.1750.149, permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto, aproveitando o manuseio inadequado de tarefas agendadas durante o desligamento de um thread.
CVE-2014-1701	A função GenerateFunction em bindings / scripts / code_generator_v8.pm no Blink, conforme usada no Google Chrome antes de 33.0.1750.149, não implementa uma restrição de origem cruzada para a função EventTarget :: dispatchEvent, que permite que atacantes remotos conduzam XSS universal (UXSS) ataques via vetores envolvendo eventos.
CVE-2014-1700	A vulnerabilidade use-after-free em modules / speech / SpeechSynthesis.cpp no Blink, usada no Google Chrome antes de 33.07.17.149, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando o manuseio impróprio de uma determinada expressão estrutura de dados.
CVE-2014-1681	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 32.07.2002 têm vetores de impacto e ataque desconhecidos, relacionadas a 12 "correções de segurança [que não foram] contribuídas por pesquisadores externos ou particularmente interessantes".
CVE-2014-1568	Serviços de Segurança de Rede Mozilla (NSS) anteriores a 3.16.2.1, 3.16.x anteriores a 3.16.5 e 3.17.x anteriores a 3.17.1, conforme utilizado no Mozilla Firefox anterior a 32.0.3, no Mozilla Firefox ESR 24.x anterior a 24.8.1 e 31.x antes de 31.1.1, Mozilla Thunderbird antes de 24.8.1 e 31.x antes de 31.1.2, Mozilla SeaMonkey antes 2.29.1, Google Chrome antes de 37.0.2062.124 no Windows e OS X e Google Chrome OS antes de 37.0.2062.120 , não analisa adequadamente os valores ASN.1 nos certificados X.509, o que torna mais fácil para os invasores remotos falsificar assinaturas RSA por meio de um certificado criado, também conhecido como um problema de "maleabilidade de assinatura".
CVE-2013-6802	O Google Chrome, anterior a 31.06.57.57, permite que atacantes remotos contornem as restrições de sandbox pretendidas, aproveitando o acesso a um processo de renderização, conforme demonstrado durante uma competição Mobile Pwn2Own na PacSec

Nome	Descrição
CVE-2013-6632	2013, uma vulnerabilidade diferente da CVE-2013-6632.
CVE-2013-6668	Várias vulnerabilidades não especificadas no Google V8 anteriores a 3.24.35.10, conforme usadas no Google Chrome antes de 33.0.1750.146, permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-6667	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 33.0.1750.146 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-6666	A função PepperFlashRendererHost :: OnNavigate no renderer / pepper / pepper_flash_renderer_host.cc no Google Chrome anterior a 33.0.1750.146 não verifica se todos os cabeçalhos são cabeçalhos simples de CORS (Cross-Origin Resource Sharing) antes de continuar com uma operação PPB_Flash.Navigate, o que pode permitir atacantes remotos para contornar restrições CORS pretendidas através de um cabeçalho inadequado.
CVE-2013-6665	O estouro de buffer com base em heap na função ResourceProvider :: InitializeSoftware em cc / resources / resource_provider.cc no Google Chrome antes de 33.0.1750.146 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um tamanho de textura grande que provoque erros alocação de memória no renderizador de software.
CVE-2013-6664	A vulnerabilidade use-after-free na função FormAssociatedElement :: formRemovedFromTree no core / html / FormAssociatedElement.cpp no Blink, conforme usada no Google Chrome antes de 33.0.1750.146, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores envolvendo elementos FORM, como demonstrado pelo uso do recurso de reconhecimento de fala.
CVE-2013-6663	A vulnerabilidade "usar-depois-livre" na função SVGImage :: setContainerSize no core / svg / graphics / SVGImage.cpp na implementação do SVG no Blink, usada no Google Chrome antes de 33.0.1750.146, permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto através de vetores relacionados ao redimensionamento de uma visão.
CVE-2013-6662	O Google Chrome armazena em cache as sessões de TLS antes da validação do certificado.
CVE-2013-6661	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 33.07.750.117 permitem que os invasores ignorem o mecanismo de proteção de sandbox após obter o acesso do renderizador ou ter outro impacto por meio de vetores desconhecidos.
CVE-2013-6660	A implementação de arrastar e soltar no Google Chrome anterior a 33.07.750.117 não restringe adequadamente as informações nas

Nome	Descrição
CVE-2013-6659	estruturas de dados WebDropData, o que permite que atacantes remotos descubram nomes completos de caminho por meio de um site criado.
CVE-2013-6659	A função SSLClientSocketNSS :: Core :: OwnAuthCertHandler em net / socket / ssl_client_socket_nss.cc no Google Chrome antes de 33.0.1750.117 não impede alterações nos certificados X.509 do servidor durante renegociações, o que permite que os servidores SSL remotos açãoem o uso de uma nova cadeia de certificados , inconsistente com as expectativas do usuário, iniciando uma renegociação TLS.
CVE-2013-6658	Várias vulnerabilidades de uso livre na implementação de layout no Blink, usadas no Google Chrome antes de 33.07.750.117, permitem que atacantes remotos causem uma negação de serviço ou possivelmente não tenham outro impacto causado por vetores envolvendo (1) executar código JavaScript durante a execução da função updateWidgetPositions ou (2) fazendo uma chamada em um plugin durante a execução da função updateWidgetPositions.
CVE-2013-6657	core / html / parser / XSSAuditor.cpp no auditor XSS no Blink, conforme usado no Google Chrome antes de 33.07.750.117, insere o URL about: blank durante determinado bloqueio de elementos FORM dentro de solicitações HTTP, o que permite que atacantes remotos contornem a mesma Política de Origem e obter informações confidenciais através de vetores não especificados.
CVE-2013-6656	A função XSSAuditor :: init no core / html / parser / XSSAuditor.cpp no auditor do XSS no Blink, conforme usada no Google Chrome antes de 33.07.750.117, processa solicitações de POST usando o corpo de uma página de redirecionamento em vez do corpo de uma meta de redirecionamento, que permite que atacantes remotos obtenham informações confidenciais por meio de vetores não especificados.
CVE-2013-6655	A vulnerabilidade use-after-free no Blink, usada no Google Chrome antes de 33.07.750.117, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio inadequado de eventos DOM substituídos durante a interação entre JavaScript e layout .
CVE-2013-6654	A função SVGAnimateElement :: calculateAnimatedValue no core / svg / SVGAnimateElement.cpp no Blink, conforme usada no Google Chrome antes de 33.0.1750.117, não lida corretamente com tipos de dados inesperados, o que permite que atacantes remotos causem uma negação de serviço (conversão incorreta) ou possivelmente não especificou outro impacto através de vetores desconhecidos.
CVE-2013-6653	A vulnerabilidade "usar-depois-livre" na implementação do conteúdo da Web no Google Chrome anterior a 33.07.750.117 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de

Nome	Descrição
	vetores que envolvam acesso conflituoso ao seletor de cores.
CVE-2013-6652	A vulnerabilidade de travessia de diretório no sandbox / win / src / named_pipe_dispatcher.cc no Google Chrome anterior a 33.0.1750.117 no Windows permite que invasores contornem as restrições de diretiva de pipe nomeado na caixa de proteção por meio de vetores relacionados a (1) falta de verificações para ponto) seqüências ou (2) falta de uso do mecanismo de proteção \\?.
CVE-2013-6650	A função StoreBuffer :: ExemptPopularPages em store-buffer.cc no Google V8 anterior a 22.03.24.16, conforme usada no Google Chrome antes de 32.07.2002, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam o manuseio incorreto de "páginas populares".
CVE-2013-6649	A vulnerabilidade use-after-free na função RenderSVGImage :: paint no core / rendering / svg / RenderSVGImage.cpp no Blink, como usada no Google Chrome antes de 32.0.1700.102, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outros não especificados. impacto através de vetores envolvendo uma imagem SVG de tamanho zero.
CVE-2013-6647	Um uso depois de livre em AnimationController :: endAnimationUpdate no Google Chrome.
CVE-2013-6646	A vulnerabilidade "usar-depois-livre" na implementação do Web Workers no Google Chrome antes de 32.0.1700.76 no Windows e antes de 32.0.1700.77 no Mac OS X e Linux permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados a o encerramento de um processo de trabalho.
CVE-2013-6645	A vulnerabilidade "use-after-free" na função OnWindowRemovingFromRootWindow em content / browser / web_contents / web_contents_view_aura.cc no Google Chrome antes de 32.0.1700.76 no Windows e antes de 32.0.1700.77 no Mac OS X e Linux permite que invasores remotos assistidos por usuários causem uma negação de serviço ou possivelmente não ter especificado outro impacto por meio de vetores que envolvem determinadas ações de visualização de impressão e de troca de guias que interagem com um elemento de entrada de fala.
CVE-2013-6644	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 32.0.1700.76 no Windows e anteriores a 32.0.1700.77 no Mac OS X e no Linux permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-6643	A função OneClickSigninBubbleView :: WindowClosing no navegador / ui / views / sync / one_click_signin_bubble_view.cc no Google Chrome antes de 32.0.1700.76 no Windows e antes de 32.0.1700.77 no Mac OS X e Linux permite que os invasores açãoem uma sincronização com uma conta do Google arbitrária

Nome	Descrição
	aproveitando o manuseio inadequado do fechamento de uma caixa de diálogo de confirmação de conexão não confiável.
CVE-2013-6642	O Google Chrome até o 32.0.1700.23 no Android permite que atacantes remotos falsifiquem a barra de endereço por meio de vetores não especificados.
CVE-2013-6641	A vulnerabilidade use-after-free na função FormAssociatedElement :: formRemovedFromTree no core / html / FormAssociatedElement.cpp no Blink, conforme usada no Google Chrome antes de 32.0.1700.76 no Windows e antes de 32.0.1700.77 no Mac OS X e Linux, permite que invasores remotos causar uma negação de serviço ou possivelmente ter outro impacto não especificado, aproveitando o tratamento incorreto do mapa de nomes anteriores de um elemento FORM.
CVE-2013-6640	A função DehoistArrayIndex em hydrogen-dehoist.cc (aka hydrogen.cc) no Google V8 anterior a 3.22.24.7, como usada no Google Chrome antes de 31.0.1650.63, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) via código JavaScript que define uma variável para o valor de um elemento de matriz com um índice criado.
CVE-2013-6639	A função DehoistArrayIndex em hydrogen-dehoist.cc (aka hydrogen.cc) no Google V8 anterior a 3.22.24.7, como usada no Google Chrome antes de 31.0.1650.63, permite que atacantes remotos causem uma negação de serviço (gravação fora do limite) ou possivelmente não especificou outro impacto via código JavaScript que define o valor de um elemento de matriz com um índice criado.
CVE-2013-6638	Vários estouros de buffer no runtime.cc no Google V8 anteriores a 3.22.24.7, conforme usados no Google Chrome antes de 31.06.1650,63, permitem que atacantes remotos causem uma negação de serviço ou possam ter outro impacto não especificado por meio de vetores que acionam uma grande matriz tipificada relacionada para as funções (1) Runtime_TypedArrayInitialize e (2) Runtime_TypedArrayInitializeFromArrayLike.
CVE-2013-6637	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 31.06.1650 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-6636	A função FrameLoader :: notifyIfInitialDocumentAccessed no core / loader / FrameLoader.cpp no Blink, como usada no Google Chrome antes de 31.0.1650.63, faz uma verificação incorreta de um documento vazio durante a apresentação de um diálogo modal, que permite que invasores remotos falsifiquem o endereço barra via vetores envolvendo o método document.write.
CVE-2013-6635	A vulnerabilidade de uso após a liberação na implementação de edição no Blink, usada no Google Chrome antes de 31.06.1650, permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via código

Nome	Descrição
	JavaScript que aciona a remoção de um nó durante o processamento a árvore DOM, relacionada a CompositeEditCommand.cpp e ReplaceSelectionCommand.cpp.
CVE-2013-6634	A função OneClickSigninHelper :: ShowInfoBarIfPossible no navegador / ui / sync / one_click_signin_helper.cc no Google Chrome anterior a 31.0.1650.63 usa uma URL incorreta durante a validação do território, que permite que atacantes remotos realizem ataques de fixação de sessão e seqüestrem sessões da Web acionando sincronização incorreta após um Código de status HTTP 302 (também conhecido como Encontrado).
CVE-2013-6632	O estouro de inteiro no Google Chrome antes de 31.0.1650.57 permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados, conforme demonstrado durante uma competição Mobile Pwn2Own na PacSec 2013.
CVE-2013-6631	A vulnerabilidade use-after-free na função Channel :: SendRTCPPacket em voice_engine / channel.cc na libjingle no WebRTC, como usada no Google Chrome antes de 31.0.1650.48 e outros produtos, permite que atacantes remotos causem uma negação de serviço (corrupção de memória de heap) ou possivelmente não especificou outro impacto através de vetores que acionam a ausência de certas inicializações estatísticas, levando ao salto de uma chamada requerida de DeRegisterExternalTransport.
CVE-2013-6630	A função get_dht no jdmarker.c no libjpeg-turbo através de 1.3.0, como usada no Google Chrome antes de 31.0.1650.48 e outros produtos, não define todos os elementos de um determinado array de valores de Huffman durante a leitura dos segmentos que seguem Definir Tabela de Huffman Marcadores JPEG (DHT), que permitem que atacantes remotos obtenham informações confidenciais de locais de memória não inicializados por meio de uma imagem JPEG criada.
CVE-2013-6629	A função get_sos no jdmarker.c em (1) libjpeg 6b e (2) libjpeg-turbo até a 1.3.0, como usada no Google Chrome antes de 31.0.1650.48, Ghostscript e outros produtos, não verifica certas duplicações de dados de componentes durante a leitura de segmentos que seguem os marcadores JPEG Start Of Scan (SOS), que permitem que atacantes remotos obtenham informações confidenciais de locais de memória não inicializados por meio de uma imagem JPEG criada.
CVE-2013-6628	net / socket / ssl_client_socket_nss.cc na implementação de TLS no Google Chrome antes de 31.0.1650.48 não garante que o certificado X.509 de um servidor seja o mesmo durante a renegociação como era antes da renegociação, o que pode permitir que servidores remotos interfiram nas relações de confiança renegociando uma sessão.
CVE-2013-6627	net / http / http_stream_parser.cc no Google Chrome anterior a 31.0.1650.48 não processa adequadamente códigos de status

Nome	Descrição
	HTTP Informativos (também conhecidos como 1xx), o que permite que servidores remotos causem uma negação de serviço (leitura fora dos limites) por meio de uma resposta preparada .
CVE-2013-6626	A função WebContentsImpl :: AttachInterstitialPage em content / browser / web_contents / web_contents_impl.cc no Google Chrome anterior a 31.0.1650.48 não cancela as caixas de diálogo JavaScript ao gerar um aviso de interstitial, que permite que atacantes remotos falsifiquem a barra de endereço por meio de um site criado.
CVE-2013-6625	A vulnerabilidade use-after-free no core / dom / ContainerNode.cpp no Blink, usada no Google Chrome antes de 31.0.1650.48, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando o manuseio inadequado de objetos de intervalo DOM em circunstâncias que exijam a remoção do nó filho após uma (1) mutação ou (2) evento de desfoque.
CVE-2013-6624	A vulnerabilidade de uso após a liberação no Google Chrome antes de 31.0.1650.48 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo os valores de string dos atributos id.
CVE-2013-6623	A implementação do SVG no Blink, como usada no Google Chrome antes de 31.0.1650.48, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) aproveitando o uso da ordem de árvore, em vez da ordem de dependência transitiva, para o layout.
CVE-2013-6622	A vulnerabilidade use-after-free na função HTMLMediaElement :: didMoveToNewDocument no core / html / HTMLMediaElement.cpp no Blink, conforme usada no Google Chrome antes de 31.0.1650.48, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem o movimento de um elemento de mídia entre documentos.
CVE-2013-6621	A vulnerabilidade "usar-depois-livre" no Google Chrome até 31.0.1650.48 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao atributo x-webkit-speech em um elemento INPUT de texto.
CVE-2013-6166	O Google Chrome antes de 29 envia cabeçalhos de cookies HTTP sem primeiro validar que eles têm as restrições de conjunto de caracteres necessárias, o que permite que invasores remotos realizem o equivalente a um ataque CSRF de logout persistente por meio de um parâmetro criado que force um aplicativo da Web a definir um cookie malformado uma resposta HTTP.
CVE-2013-2931	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 31.0.1650.48 permitem que os invasores executem código arbitrário ou possivelmente tenham outro impacto por meio

Nome	Descrição
	de vetores desconhecidos.
CVE-2013-2928	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 30.0.1599.101 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2927	A vulnerabilidade use-after-free na função <code>HTMLFormElement :: prepareForSubmission</code> no <code>core / html / HTMLFormElement.cpp</code> no Blink, conforme usada no Google Chrome antes de 30.0.1599.101, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à submissão de elementos FORM.
CVE-2013-2926	A vulnerabilidade use-after-free na função <code>IndentOutdentCommand :: tryIndentingAsListItem</code> no <code>core / editing / IndentOutdentCommand.cpp</code> no Blink, como usada no Google Chrome antes de 30.0.1599.101, permite que atacantes remotos assistidos por usuário causem uma negação de serviço ou possivelmente não tenham especificado outro impacto através de vetores relacionados aos elementos da lista.
CVE-2013-2925	A vulnerabilidade use-after-free no <code>core / xml / XMLHttpRequest.cpp</code> no Blink, usada no Google Chrome antes de 30.0.1599.101, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que açãoam vários usos conflitantes de o mesmo objeto XMLHttpRequest.
CVE-2013-2924	A vulnerabilidade "use-after-free" no International Components for Unicode (ICU), usada no Google Chrome antes de 30.0.1599.66 e em outros produtos, permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2923	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 30.0.1599.66 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2922	A vulnerabilidade use-after-free no <code>core / html / HTMLTemplateElement.cpp</code> no Blink, usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que opera em um Elemento de modelo.
CVE-2013-2921	A vulnerabilidade livre dupla na função <code>ResourceFetcher :: didLoadResource</code> no <code>core / fetch / ResourceFetcher.cpp</code> no carregador de recursos no Blink, conforme usado no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado açãoando determinado processamento de retorno de chamada durante o relatório de uma entrada de recurso.

Nome	Descrição
CVE-2013-2920	A função DoResolveRelativeHost em url / url_canon_relative.cc no Google Chrome anterior a 30.0.1599.66 permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de um URL relativo contendo um nome de host, conforme demonstrado por um URL relativo a protocolo. com uma //www.google.com/string.
CVE-2013-2919	O Google V8, usado no Google Chrome antes de 30.0.1599.66, permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente não tenham outro impacto desconhecido por meio de vetores desconhecidos.
CVE-2013-2918	A vulnerabilidade use-after-free na função RenderBlock :: collapseAnonymousBlockChild em core / rendering / RenderBlock.cpp na implementação DOM no Blink, como usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham Outro impacto não especificado, aproveitando o tratamento incorreto de relacionamentos pai-filho para blocos anônimos.
CVE-2013-2917	A função ReverbConvolverStage :: ReverbConvolverStage no core / platform / audio / ReverbConvolverStage.cpp na implementação do Web Audio no Blink, usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites)) através de vetores relacionados ao array impulseResponse.
CVE-2013-2916	O Blink, usado no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos falsifiquem a barra de endereços por meio de vetores que envolvam uma resposta com um código de status 204 (também conhecido como Sem conteúdo), juntamente com um atraso na notificação do usuário de uma tentativa de falsificação.
CVE-2013-2915	O Google Chrome anterior a 30.0.1599.66 preserva objetos NavigationEntry pendentes em determinadas circunstâncias inválidas, o que permite que atacantes remotos falsifiquem a barra de endereços por meio de um URL com um esquema malformado, conforme demonstrado por um URL inexistente: 12121.
CVE-2013-2914	A vulnerabilidade "usar-depois-livre" no diálogo de escolha de cores no Google Chrome antes de 30.0.1599.66 no Windows permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a color_chooser_dialog.cc e color_chooser_win.cc no navegador / ui / views /.
CVE-2013-2913	A vulnerabilidade use-after-free na função XMLDocumentParser :: append no core / xml / parser / XMLDocumentParser.cpp no Blink, como usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outros não especificados. impacto através de vetores envolvendo um documento XML.
CVE-2013-2912	A vulnerabilidade use-after-free na função PepperInProcessRouter

Nome	Descrição
CVE-2013-2911	:: SendToHost em content / renderer / pepper / pepper_in_process_router.cc na API do Plug-in da Pepper (PPAPI) no Google Chrome antes de 30.0.1599.66 permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto através de vetores envolvendo uma mensagem de destruição de recursos.
CVE-2013-2910	A vulnerabilidade use-after-free na função XSLStyleSheet :: compileStyleSheet no core / xml / XSLStyleSheetLibxslt.cpp no Blink, como usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado aproveitando o manuseio inadequado da recompilação pós-falha em versões libxslt não especificadas.
CVE-2013-2909	A vulnerabilidade use-after-free nos módulos / webaudio / AudioScheduledSourceNode.cpp na implementação do Web Audio no Blink, usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos .
CVE-2013-2908	A vulnerabilidade de uso após a liberação no Blink, usada no Google Chrome antes de 30.0.1599.66, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à renderização de bloco inline para texto Unicode bidirecional em um elemento isolado de seus irmãos.
CVE-2013-2907	O Google Chrome anterior a 30.0.1599.66 usa chamadas de função incorretas para determinar os valores dos objetos NavigationEntry, o que permite que atacantes remotos falsifiquem a barra de endereço por meio de vetores que envolvam uma resposta com um código de status 204 (também conhecido como Sem conteúdo).
CVE-2013-2906	A implementação do objeto Window.prototype no Google Chrome anterior a 30.0.1599.66 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2013-2905	Várias condições de corrida na implementação do Web Audio no Blink, usadas no Google Chrome antes de 30.0.1599.66, permitem que atacantes remotos causem uma negação de serviço ou possivelmente não tenham outro impacto por meio de vetores relacionados ao encadeamento no core / html / HTMLMediaElement.cpp, core / platform / audio / AudioDSPKernelProcessor.cpp, núcleo / plataforma / áudio / HRTFElevation.cpp e módulos / webaudio / ConvolverNode.cpp.
CVE-2013-2905	A função SharedMemory :: Create em memory / shared_memory_posix.cc no Google Chrome anterior a 29.0.1547.57 usa permissões fracas em / dev / shm /, o que permite que os invasores obtenham informações confidenciais por meio do acesso direto a um arquivo de memória compartilhada POSIX.

Nome	Descrição
CVE-2013-2904	A vulnerabilidade use-after-free na função Document :: finishedParsing no core / dom / Document.cpp no Blink, como usada no Google Chrome antes de 29.0.1547.57, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via um evento onload que altera um elemento IFRAME para que seu atributo src não seja mais um documento XML, levando à coleta de lixo não intencional deste documento.
CVE-2013-2903	A vulnerabilidade use-after-free na função HTMLMediaElement :: didMoveToNewDocument em core / html / HTMLMediaElement.cpp no Blink, como usada no Google Chrome antes de 29.0.1547.57, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores envolvendo a movimentação de um (1) elemento AUDIO ou (2) VIDEO entre documentos.
CVE-2013-2902	A vulnerabilidade "usar-depois-livre" na implementação do XSLT ProcessingInstruction no Blink, usada no Google Chrome antes de 29.0.1547.57, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado através de vetores relacionados a uma chamada applyXSLTransform envolvendo (1) um documento HTML ou (2) um elemento xsl: processing-instruction que ainda está no processo de carregamento.
CVE-2013-2901	Múltiplos inteiros estouraram em (1) libGLESv2 / renderer / Renderer9.cpp e (2) libGLESv2 / renderer / Renderer11.cpp no mecanismo de camada de gráficos nativos (ANGLE), como usado no Google Chrome antes de 29.0.1547.57, permitindo que atacantes remotos causem uma negação de serviço ou possivelmente não ter especificado outro impacto através de vetores desconhecidos.
CVE-2013-2900	A função FilePath :: ReferencesParent em files / file_path.cc no Google Chrome anterior a 29.0.1547.57 no Windows não lida corretamente com componentes de nome de caminho compostos inteiramente de. (ponto) e caracteres de espaço em branco, o que permite que atacantes remotos realizem ataques de passagem de diretórios por meio de um nome de diretório criado.
CVE-2013-2887	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 29.0.1547.57 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2886	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 28.0.1500.95 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2885	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 28.0.1500.95 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a não considerar

Nome	Descrição
	adequadamente o foco durante o processamento de eventos JavaScript na presença de vários campos tipo de entrada.
CVE-2013-2884	A vulnerabilidade "usar-depois-livre" na implementação do DOM no Google Chrome antes de 28.0.1500.95 permite que invasores remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados ao rastreamento inadequado de qual documento possui um objeto Attr.
CVE-2013-2883	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 28.0.1500.95 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à exclusão do registro de um objeto MutationObserver.
CVE-2013-2882	O Google V8, usado no Google Chrome antes de 28.0.1500.95, permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que geram "confusão de tipo".
CVE-2013-2881	O Google Chrome anterior a 28.0.1500.95 não processa corretamente frames, o que permite que atacantes remotos contornem a Política de mesma origem por meio de um site criado.
CVE-2013-2880	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 28.0.1500.71 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2879	O Google Chrome anterior a 28.0.1500.71 não determina adequadamente as circunstâncias em que um processo de renderizador pode ser considerado um processo confiável para login e operações de sincronização subsequentes, o que facilita para invasores remotos realizar ataques de phishing por meio de um site criado.
CVE-2013-2878	O Google Chrome anterior a 28.0.1500.71 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores relacionados ao processamento de texto.
CVE-2013-2877	parser.c em libxml2 antes de 2.9.0, como usado no Google Chrome antes de 28.0.1500.71 e outros produtos, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento que termina abruptamente, relacionado ao falta de certas verificações para o estado XML_PARSER_EOF.
CVE-2013-2876	O navegador / extensions / api / tabs / tabs_api.cc no Google Chrome anterior a 28.0.1500.71 não impõe restrições na captura de capturas de tela por extensões, o que permite que atacantes remotos obtenham informações confidenciais sobre o conteúdo de uma página anterior por meio de vetores que envolvam um página intersticial.
CVE-2013-2875	core / rendering / svg / SVGInlineTextBox.cpp na implementação do SVG no Blink, como usado no Google Chrome antes de 28.0.1500.71, permite que atacantes remotos causem uma

Nome	Descrição
CVE-2013-2874	negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2013-2873	O Google Chrome antes de 28.0.1500.71 no Windows, quando uma GPU da Nvidia é usada, permite que atacantes remotos contornem as restrições pretendidas ao acesso a dados de tela por meio de vetores que envolvem a transmissão IPC de texturas GL.
CVE-2013-2872	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 28.0.1500.71 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam um código de status HTTP 404 durante o carregamento de recursos.
CVE-2013-2871	O Google Chrome anterior ao 28.0.1500.71 no Mac OS X não garante uma fonte suficiente de entropia para os processos do renderizador, o que pode facilitar para os invasores remotos derrotarem os mecanismos de proteção criptográfica em componentes de terceiros por meio de vetores não especificados.
CVE-2013-2870	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 28.0.1500.71 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de entrada.
CVE-2013-2869	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 28.0.1500.71 permite que servidores remotos executem código arbitrário por meio de tráfego de resposta elaborado após uma solicitação de URL.
CVE-2013-2868	O Google Chrome anterior a 28.0.1500.71 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de uma imagem JPEG2000 criada.
CVE-2013-2867	common / extensions / sync_helper.cc no Google Chrome antes de 28.0.1500.71 prossegue com as operações de sincronização para extensões NPAPI sem verificar uma determinada configuração de permissão de plug-in, o que pode permitir que atacantes remotos Guy alterações indesejadas de extensão através de vetores não especificados.
CVE-2013-2867	O Google Chrome anterior a 28.0.1500.71 não impede adequadamente janelas pop-under, o que permite que invasores remotos Guy um impacto não especificado por meio de um site criado.
CVE-2013-2866	O plug-in do Flash no Google Chrome anterior a 27.0.1453.116, conforme usado no Google Chrome OS antes de 27.0.1453.116 e separadamente, não determina adequadamente se um usuário deseja permitir acesso de câmera ou microfone por um aplicativo Flash, o que permite que invasores remotos obtenha informações confidenciais do ambiente físico de uma máquina por meio de um ataque clickjacking, conforme demonstrado por um ataque usando uma propriedade de opacidade CSS (Cascading Style Sheets) trabalhada.

Nome	Descrição
CVE-2013-2865	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 27.0.1453.110 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2864	A funcionalidade PDF no Google Chrome anterior a 27.0.1453.110 permite que invasores remotos causem uma negação de serviço (operação livre inválida) ou possivelmente não tenham outro impacto específico por meio de vetores desconhecidos.
CVE-2013-2863	O Google Chrome anterior a 27.0.1453.110 não lida adequadamente com soquetes SSL, o que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados.
CVE-2013-2862	O Skia, como usado no Google Chrome antes de 27.0.1453.110, não manipula adequadamente a aceleração de GPU, que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2861	A vulnerabilidade de uso após a liberação na implementação de SVG no Google Chrome anterior a 27.0.1453.110 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2860	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 27.0.1453.110 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam acesso a uma API de banco de dados por um processo de trabalho.
CVE-2013-2859	O Google Chrome anterior a 27.0.1453.110 permite que invasores remotos contornem a Política de mesma origem e açãoem a poluição de espaço de nomes por meio de vetores não especificados.
CVE-2013-2858	A vulnerabilidade "usar-depois-de-graça" na implementação de áudio HTML5 no Google Chrome anterior a 27.0.1453.110 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2857	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 27.0.1453.110 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de imagens.
CVE-2013-2856	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 27.0.1453.110 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de entrada.

Nome	Descrição
CVE-2013-2855	A API de ferramentas para desenvolvedores do Google Chrome anterior a 27.0.1453.110 permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2854	O Google Chrome antes de 27.0.1453.110 no Windows fornece um identificador incorreto para um processo de renderização em circunstâncias não especificadas, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2853	A implementação HTTPS no Google Chrome anterior a 28.0.1500.71 não garante que os cabeçalhos sejam terminados por \r\n\r\n (retorno de carro, nova linha, retorno de carro, nova linha), o que permite que invasores intermediários tenham um impacto não especificado por meio de vetores que acionam o truncamento de cabeçalho.
CVE-2013-2849	Várias vulnerabilidades de cross-site scripting (XSS) no Google Chrome anteriores a 27.0.1453.93 permitem que atacantes remotos assistidos por usuário injetem script web ou HTML arbitrário por meio de vetores que envolvam (1) arrastar e soltar ou (2) copiar e colar Operação.
CVE-2013-2848	O Auditor XSS no Google Chrome anterior a 27.0.1453.93 pode permitir que atacantes remotos obtenham informações confidenciais por meio de vetores não especificados.
CVE-2013-2847	A condição de corrida na implementação de trabalhadores no Google Chrome antes de 27.0.1453.93 permite que atacantes remotos causem uma negação de serviço (uso após a queda livre e de aplicativo) ou possivelmente não tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2846	A vulnerabilidade "usar-depois-livre" no carregador de mídia do Google Chrome anterior a 27.0.1453.93 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos, uma vulnerabilidade diferente da CVE-2013-2840.
CVE-2013-2845	A implementação do Web Audio no Google Chrome anterior a 27.0.1453.93 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2844	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 27.0.1453.93 permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados à resolução de estilo.
CVE-2013-2843	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 27.0.1453.93 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto

Nome	Descrição
	não especificado por meio de vetores relacionados ao tratamento de dados de fala.
CVE-2013-2842	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 27.0.1453.93 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de widgets.
CVE-2013-2841	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 27.0.1453.93 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de recursos do Pepper.
CVE-2013-2840	A vulnerabilidade "usar-depois-livre" no carregador de mídia do Google Chrome anterior a 27.0.1453.93 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos, uma vulnerabilidade diferente da CVE-2013-2846.
CVE-2013-2839	O Google Chrome anterior a 27.0.1453.93 não executa adequadamente uma conversão de uma variável não especificada durante o tratamento de dados da área de transferência, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2838	O Google V8, usado no Google Chrome antes de 27.0.1453.93, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2013-2837	A vulnerabilidade de uso após a liberação na implementação de SVG no Google Chrome anterior a 27.0.1453.93 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-2836	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 27.0.1453.93 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-2835	O Google Chrome OS anterior a 26.0.1410.57 não impõe corretamente restrições de origem para os plug-ins O3D e Google Talk, o que permite que atacantes remotos ignorem o mecanismo de proteção de lista de permissões de domínio por meio de um site criado, uma vulnerabilidade diferente da CVE-2013-2834 .
CVE-2013-2834	O Google Chrome OS anterior a 26.0.1410.57 não impõe corretamente restrições de origem para os plug-ins O3D e Google Talk, o que permite que atacantes remotos ignorem o mecanismo de proteção de lista de permissões de domínio por meio de um site criado, uma vulnerabilidade diferente da CVE-2013-2835 .
CVE-2013-2833	A vulnerabilidade "usar-depois-livre" no plug-in O3D no Google Chrome OS anterior a 26.0.1410.57 permite que atacantes

Nome	Descrição
	remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao gerenciamento inadequado de relacionamentos de propriedade que envolvem elementos e DrawElements.
CVE-2013-2832	A função Buffer :: Set no core / cross / buffer.cc no plug-in do O3D no Google Chrome OS anterior a 26.0.1410.57 não impede que dados não inicializados permaneçam em um buffer, o que pode permitir que atacantes remotos obtenham informações confidenciais por meio de informações não especificadas. vetores.
CVE-2013-2632	O Google V8 anterior a 3.17.13, conforme usado no Google Chrome antes de 27.0.1444.3, permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente não tenham outro impacto específico por meio de código JavaScript criado, conforme demonstrado pelo jogo Bejeweled.
CVE-2013-2493	A função Hook_Terminate em chrome_frame / protocol_sink_wrap.cc no plug-in do Google Chrome Frame antes de 26.0.1410.28 para o Internet Explorer não manipula adequadamente as solicitações de tabulação anexadas, o que permite que atacantes remotos assistidos por usuário causem uma negação de serviço (falha do aplicativo) por meio de um _blank valor para o atributo de destino de um elemento A.
CVE-2013-2268	A vulnerabilidade não especificada na implementação MathML no WebKit no Google Chrome antes de 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X, tem vetores de impacto e ataque remoto desconhecidos, relacionados a um "problema de segurança de alta gravidade".
CVE-2013-1489	A vulnerabilidade não especificada no componente Java Runtime Environment (JRE) do Oracle Java SE 7 Update 10 e Update 11, quando executado no Windows usando o Internet Explorer, Firefox, Opera e Google Chrome, permite que atacantes remotos contornem o nível de segurança "Very High" do Java Control Panel e executar código Java não assinado sem avisar o usuário por meio de vetores desconhecidos, também conhecidos como "Issue 53" e a vulnerabilidade "Java Security Slider".
CVE-2013-0927	O Google Chrome OS anterior a 26.0.1410.57 depende de uma implementação de pango-utils.c read_config do Pango que carrega o conteúdo do arquivo .pangorc no diretório inicial do usuário e o arquivo referenciado pela variável de ambiente PANGO_RC_FILE, que permite que invasores ignorem o acesso pretendido restrições através de dados de configuração criados.
CVE-2013-0926	O Google Chrome anterior a 26.0.1410.43 não lida corretamente com conteúdo ativo em um elemento EMBED durante uma operação de copiar e colar, o que permite que invasores remotos assistidos pelo usuário tenham um impacto não especificado por meio de um site criado.
CVE-2013-0925	O Google Chrome anterior a 26.0.1410.43 não garante que uma

Nome	Descrição
	extensão tenha permissão para abas (também conhecida como APIPermission :: kTab) antes de fornecer um URL para essa extensão, que possui vetores de impacto e ataque remoto não especificados.
CVE-2013-0924	A funcionalidade de extensão no Google Chrome anterior a 26.0.1410.43 não verifica se o uso da API de permissões é consistente com as permissões de arquivo, que têm um impacto não especificado e vetores de ataque.
CVE-2013-0923	A API de aplicativos USB do Google Chrome anterior a 26.0.1410.43 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados.
CVE-2013-0922	O Google Chrome anterior a 26.0.1410.43 não restringe adequadamente as tentativas de acesso a força bruta contra sites que exigem Autenticação Básica HTTP, que possui vetores de impacto e de ataque não especificados.
CVE-2013-0921	O recurso Sites isolados no Google Chrome anterior a 26.0.1410.43 não impõe adequadamente o uso de processos separados, o que facilita para invasores remotos evitar as restrições de acesso pretendidas por meio de um site criado.
CVE-2013-0920	A vulnerabilidade de uso após a liberação na API de marcadores de extensão no Google Chrome anterior a 26.0.1410.43 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-0919	A vulnerabilidade de uso após a liberação no Google Chrome antes de 26.0.1410.43 no Linux permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado ao aproveitar a presença de uma extensão que cria uma janela pop-up.
CVE-2013-0918	O Google Chrome anterior a 26.0.1410.43 não impede a navegação para ferramentas de desenvolvedor em resposta a uma operação de arrastar e soltar, que permite que invasores remotos assistidos por usuários tenham um impacto não especificado por meio de um site criado.
CVE-2013-0917	O carregador de URLs no Google Chrome anterior a 26.0.1410.43 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2013-0916	A vulnerabilidade "usar-depois-livre" na implementação do Web Audio no Google Chrome antes de 26.0.1410.43 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-0915	O processo de GPU no Google Chrome OS anterior a 25.03.13.173 permite que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a um "estouro".

Nome	Descrição
CVE-2013-0913	Incremento de inteiro nos drivers / gpu / drm / i915 / i915_gem_execbuffer.c no driver i915 no subsistema Direct Rendering Manager (DRM) no kernel do Linux por meio de 3.8.3, conforme usado no Google Chrome OS anterior a 25.0.1364.173 e outros produtos, permite que os usuários locais causem uma negação de serviço (estouro de buffer baseado em heap) ou possivelmente tenham outro impacto não especificado por meio de um aplicativo criado que aciona muitas cópias de realocação e potencialmente leva a uma condição de corrida.
CVE-2013-0912	O WebKit no Google Chrome anterior a 25.0.1364.160 permite que atacantes remotos executem código arbitrário por meio de vetores que geram "confusão de tipo".
CVE-2013-0911	A vulnerabilidade de travers de diretório no Google Chrome anterior a 25.0.1364.152 permite que invasores remotos tenham um impacto não especificado por meio de vetores relacionados a bancos de dados.
CVE-2013-0910	O Google Chrome anterior a 25.0.1364.152 não gerencia adequadamente a interação entre o processo do navegador e os processos do renderizador durante a autorização do carregamento de um plug-in, o que facilita aos invasores remotos evitar as restrições de acesso pretendidas por meio de vetores que envolvam um plug-in bloqueado .
CVE-2013-0909	O Auditor XSS no Google Chrome anterior a 25.0.1364.152 permite que atacantes remotos obtenham informações sensíveis do Referenciador HTTP através de vetores não especificados.
CVE-2013-0908	O Google Chrome anterior a 25.0.1364.152 não gerencia adequadamente as ligações de processos de extensão, que têm vetores de impacto e de ataque não especificados.
CVE-2013-0907	A condição de corrida no Google Chrome anterior a 25.0.1364.152 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de segmentos de mídia.
CVE-2013-0906	A implementação do IndexedDB no Google Chrome antes de 25.0.1364.152 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-0905	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 25.0.1364.152 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo uma animação SVG.
CVE-2013-0904	A implementação do Web Audio no Google Chrome antes de 25.0.1364.152 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.

Nome	Descrição
CVE-2013-0903	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 25.0.1364.152 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio da navegação do navegador.
CVE-2013-0902	A vulnerabilidade de uso após a liberação na implementação do carregador de quadros no Google Chrome antes de 25.0.1364.152 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-0900	A condição de corrida na funcionalidade Componentes Internacionais para Unicode (ICU) no Google Chrome anterior a 25.0.1.364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que atacantes remotos causem uma negação de serviço ou possam ter outro impacto não especificado por meio de vetores desconhecidos.
CVE-2013-0899	O estouro de inteiro na implementação de preenchimento na função opus_packet_parse_impl em src / opus_decoder.c no Opus anterior à 1.0.2, conforme usado no Google Chrome antes de 25.0.1364.97 no Windows e Linux e antes de 25.0.1364.99 no Mac OS X e outros produtos, permite atacantes remotos para causar uma negação de serviço (leitura fora dos limites) através de um pacote longo.
CVE-2013-0898	A vulnerabilidade "usar-depois-livre" no Google Chrome antes de 25.03.364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores envolvendo um URL.
CVE-2013-0897	O erro "off-by-one" na funcionalidade do PDF no Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que atacantes remotos causem uma negação de serviço por meio de um documento criado.
CVE-2013-0896	O Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X não gerencia adequadamente a memória durante o tratamento de mensagens para plug-ins, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente outro impacto não especificado via vetores desconhecidos.
CVE-2013-0895	O Google Chrome anterior a 25.0.1.364.97 no Linux e antes de 25.0.1364.99 no Mac OS X não lida corretamente com nomes de caminho durante operações de cópia, o que pode facilitar a execução de programas arbitrários por vetores não especificados por invasores remotos.
CVE-2013-0894	Estouro de buffer na função vorbis_parse_setup_hdr_floors no decodificador Vorbis em vorbisdec.c no libavcodec no FFmpeg através de 1.1.3, como usado no Google Chrome antes de 25.0.1364.97 no Windows e Linux e antes de 25.0.1364.99 no Mac

Nome	Descrição
CVE-2013-0893	OS X e outros produtos, permite atacantes remotos para causar uma negação de serviço (erro de divisão por zero ou acesso a matriz fora dos limites) ou possivelmente ter outro impacto não especificado através de vetores envolvendo um valor zero para um tamanho de mapa de casca.
CVE-2013-0892	A condição de corrida no Google Chrome antes de 25.0.1364.97 no Windows e no Linux, e antes de 25.0.1364.99 no Mac OS X, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à mídia.
CVE-2013-0891	Várias vulnerabilidades não especificadas na camada IPC no Google Chrome antes de 25.0.1.364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permitem que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2013-0890	O estouro de número inteiro no Google Chrome antes de 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um blob.
CVE-2013-0889	Várias vulnerabilidades não especificadas na camada IPC no Google Chrome anteriores a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permitem que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto por meio de vetores desconhecidos .
CVE-2013-0888	O Google Chrome anterior a 25.0.1.364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X não aplica adequadamente um requisito de gesto do usuário antes de prosseguir com o download de um arquivo, o que facilita a execução de código arbitrário por invasores remotos. arquivo trabalhado.
CVE-2013-0887	O Skia, usado no Google Chrome antes de 25.0.1364.97 no Windows e no Linux, e antes de 25.0.1364.99 no Mac OS X, permite que atacantes remotos causem uma negação de serviço (leituras fora dos limites) por meio de vetores relacionados a um "usuário verificação de gesto para downloads de arquivos perigosos. "
CVE-2013-0886	O processo de ferramentas do desenvolvedor no Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X não restringe adequadamente os privilégios durante a interação com um servidor conectado, que possui vetores de impacto e de ataque não especificados.
CVE-2013-0885	O Google Chrome anterior a 25.0.1364.99 no Mac OS X não implementa adequadamente o processamento de sinal para o código Native Client (também conhecido como NaCl), que possui vetores de impacto e ataque não especificados.
	O Google Chrome anterior a 25.0.1364.97 no Windows e no Linux

Nome	Descrição
	e antes de 25.0.1364.99 no Mac OS X não restringe adequadamente os privilégios da API durante a interação com a Chrome Web Store, que possui vetores de impacto e ataque não especificados.
CVE-2013-0884	O Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X não carrega adequadamente o código Native Client (aka NaCl), que possui vetores de impacto e de ataque não especificados.
CVE-2013-0883	O Skia, usado no Google Chrome antes de 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X, permite que atacantes remotos causem uma negação de serviço (operação de leitura incorreta) por meio de vetores não especificados.
CVE-2013-0882	O Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que invasores remotos causem uma negação de serviço (acesso incorreto à memória) ou possivelmente tenham outro impacto não especificado por meio de um grande número de parâmetros SVG.
CVE-2013-0881	O Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que invasores remotos causem uma negação de serviço (operação de leitura incorreta) por meio de dados criados no formato do contêiner Matroska.
CVE-2013-0880	A vulnerabilidade de uso após a liberação no Google Chrome antes de 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X permite que atacantes remotos causem uma negação de serviço ou possivelmente não tenham outro impacto por meio de vetores relacionados a bancos de dados.
CVE-2013-0879	O Google Chrome anterior a 25.0.1364.97 no Windows e no Linux e antes de 25.0.1364.99 no Mac OS X não implementa adequadamente os nós de áudio da Web, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou tenham outro impacto não especificado vetores desconhecidos.
CVE-2013-0843	content / renderer / media / webrtc_audio_renderer.cc no Google Chrome antes de 24.0.1312.56 no Mac OS X não usa um tamanho de buffer apropriado para a taxa de amostragem de 96 kHz, que permite que atacantes remotos causem uma negação de serviço (corrupção de memória e falha de aplicativo) ou possivelmente não especificou outro impacto através de um site que fornece áudio WebRTC.
CVE-2013-0842	O Google Chrome anterior a 24.0.1312.56 não lida corretamente com% 00 caracteres em nomes de caminho, o que tem um impacto não especificado e vetores de ataque.
CVE-2013-0841	O erro de índice de matriz na funcionalidade de bloqueio de conteúdo no Google Chrome anterior a 24.0.1312.56 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de

Nome	Descrição
	vetores desconhecidos.
CVE-2013-0840	O Google Chrome anterior a 24.0.1312.56 não valida URLs durante a abertura de novas janelas, que têm vetores de impacto e ataque remoto não especificados.
CVE-2013-0839	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 24.0.1312.56 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de fontes em elementos CANVAS.
CVE-2013-0838	O Google Chrome anterior ao 24.0.1312.52 no Linux usa permissões fracas para segmentos de memória compartilhada, que têm impacto não especificado e vetores de ataque.
CVE-2013-0837	O Google Chrome anterior a 24.0.1312.52 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à manipulação de guias de extensão.
CVE-2013-0836	O Google V8 anterior a 3.14.5.3, conforme usado no Google Chrome antes de 24.0.1312.52, não implementa corretamente a coleta de lixo, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado.
CVE-2013-0835	A vulnerabilidade não especificada na implementação da Geolocalização no Google Chrome anterior a 24.0.1312.52 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores desconhecidos.
CVE-2013-0834	O Google Chrome anterior a 24.0.1312.52 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores envolvendo glifos.
CVE-2013-0833	O Google Chrome anterior a 24.0.1312.52 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores relacionados à impressão.
CVE-2013-0832	A vulnerabilidade de uso após a liberação no Google Chrome antes de 24.0.1312.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à impressão.
CVE-2013-0831	A vulnerabilidade de travers de diretório no Google Chrome anterior a 24.0.1312.52 permite que invasores remotos tenham um impacto não especificado, aproveitando o acesso a um processo de extensão.
CVE-2013-0830	A camada IPC no Google Chrome anterior a 24.0.1312.52 no Windows omite um caractere NUL necessário para o encerramento de uma estrutura de dados não especificada, que tem impacto e vetores de ataque desconhecidos.
CVE-2013-0829	O Google Chrome anterior a 24.0.1312.52 não mantém adequadamente os metadados do banco de dados, o que permite

Nome	Descrição
	que atacantes remotos contornem as restrições de acesso a arquivos desejadas por meio de vetores não especificados.
CVE-2013-0828	A funcionalidade PDF no Google Chrome anterior a 24.0.1312.52 não executa adequadamente um elenco de uma variável não especificada durante o processamento da raiz da árvore de estrutura, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado .
CVE-2012-5851	html / parser / XSSAuditor.cpp no WebCore no WebKit, conforme usado no Google Chrome até o 22 e no Safari 5.1.7, não considera todos os possíveis contextos de saída dos dados refletidos, o que facilita para invasores remotos ignorar um script entre sites (XSS) mecanismo de proteção através de uma seqüência de caracteres criados, também conhecido como problema rdar 12019108.
CVE-2012-5376	A implementação da comunicação entre processos (IPC) no Google Chrome antes de 22.0.1229.94 permite que atacantes remotos contornem as restrições de sandbox pretendidas e escrevam em arquivos arbitrários, aproveitando o acesso a um processo de renderização, uma vulnerabilidade diferente da CVE-2012-5112.
CVE-2012-5157	O Google Chrome anterior a 24.0.1312.52 não processa adequadamente dados de imagens em documentos PDF, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento criado.
CVE-2012-5156	A vulnerabilidade de uso após a liberação no Google Chrome antes de 24.0.1312.52 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo campos PDF.
CVE-2012-5155	O Google Chrome anterior ao 24.0.1312.52 no Mac OS X não usa uma abordagem de área restrita apropriada para processos de trabalho, o que facilita para invasores remotos evitar as restrições de acesso pretendidas por meio de vetores não especificados.
CVE-2012-5154	O estouro de número inteiro no Google Chrome antes de 24.0.1312.52 no Windows permite que invasores causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à alocação de memória compartilhada.
CVE-2012-5153	O Google V8 anterior a 3.14.5.3, conforme usado no Google Chrome antes de 24.0.1312.52, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que acione um acesso fora do limite à memória da pilha.
CVE-2012-5152	O Google Chrome anterior a 24.0.1312.52 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores que envolvam operações de busca em dados de vídeo.
CVE-2012-5151	O estouro de número inteiro no Google Chrome antes de 24.0.1312.52 permite que invasores remotos causem uma negação

Nome	Descrição
	de serviço ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado em um documento PDF.
CVE-2012-5150	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 24.0.1312.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam operações de busca em dados de vídeo.
CVE-2012-5149	O estouro de número inteiro na camada de IPC de áudio no Google Chrome antes de 24.0.1312.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-5148	A funcionalidade de hifenização no Google Chrome anterior a 24.0.1312.52 não valida corretamente os nomes de arquivos, que têm um impacto não especificado e vetores de ataque.
CVE-2012-5147	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 24.0.1312.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio do DOM.
CVE-2012-5146	O Google Chrome anterior a 24.0.1312.52 permite que atacantes remotos contornem a Política de mesma origem por meio de um URL malformado.
CVE-2012-5145	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 24.0.1312.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao layout do SVG.
CVE-2012-5144	O Google Chrome anterior a 23.0.1271.97 e o Libav 0.7.x anterior a 0.7.7 e 0.8.x anterior a 0.8.5, não executam corretamente a decodificação AAC, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória de pilha) ou possivelmente Outro impacto não especificado através de vetores relacionados a "uma substituição off-by-one ao alternar para o perfil LTP da MAIN".
CVE-2012-5143	O estouro de número inteiro no Google Chrome anterior a 23.0.1271.97 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a buffers de imagem PPAPI.
CVE-2012-5142	O Google Chrome anterior a 23.0.1271.97 não lida corretamente com a navegação de histórico, o que permite que invasores remotos executem código arbitrário ou causem uma negação de serviço (falha de aplicativo) por meio de vetores não especificados.
CVE-2012-5141	O Google Chrome anterior a 23.0.1271.97 não restringe adequadamente a instanciação do plug-in do cliente Chromoting, que possui vetores de impacto e ataque não especificados.

Nome	Descrição
CVE-2012-5140	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.97 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao URL loader.
CVE-2012-5139	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.97 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a eventos de visibilidade.
CVE-2012-5138	O Google Chrome anterior a 23.0.1271.95 não lida corretamente com caminhos de arquivos, que têm vetores de impacto e de ataque não especificados.
CVE-2012-5137	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.95 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à API de origem de mídia.
CVE-2012-5136	O Google Chrome anterior a 23.0.1271.91 não executa adequadamente uma conversão de uma variável não especificada durante o tratamento do elemento INPUT, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento HTML criado.
CVE-2012-5135	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.91 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à impressão.
CVE-2012-5134	O estouro de buffer baseado em heap na função xmlParseAttValueComplex no parser.c na libxml2 2.9.0 e anterior, conforme usado no Google Chrome antes de 23.0.1271.91 e outros produtos, permite que atacantes remotos causem uma negação de serviço ou possivelmente executem código arbitrário por meio de execução entidades em um documento XML.
CVE-2012-5133	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.91 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a filtros SVG.
CVE-2012-5132	O Google Chrome anterior a 23.0.1271.91 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de uma resposta com codificação de transferência em partes.
CVE-2012-5131	O Google Chrome anterior a 23.0.1271.91 no Mac OS X não atenua adequadamente o comportamento inadequado de renderização no driver da GPU Intel, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-5130	O Skia, usado no Google Chrome antes de 23.0.1271.91, permite que atacantes remotos causem uma negação de serviço (leitura

Nome	Descrição
	fora dos limites) por meio de vetores não especificados.
CVE-2012-5129	O estouro de buffer com base em heap no subsistema WebGL no Google Chrome OS anterior a 23.0.1271.94 permite que invasores remotos causem uma negação de serviço (falha do processo da GPU) ou possivelmente não tenham outro impacto por meio de vetores desconhecidos.
CVE-2012-5128	O Google V8 anterior ao 3.13.7.5, conforme usado no Google Chrome antes de 23.0.1271.64, não realiza operações de gravação corretamente, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-5127	O estouro de número inteiro no Google Chrome anterior a 23.0.1271.64 permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) ou, possivelmente, não tenham outro impacto não especificado por meio de uma imagem de WebP criada.
CVE-2012-5126	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.64 permite que invasores remotos causem uma negação de serviço ou possam ter outro impacto não especificado por meio de vetores relacionados ao manuseio de marcadores de plug-in.
CVE-2012-5125	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.64 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à manipulação de guias de extensão.
CVE-2012-5124	O Google Chrome anterior a 23.0.1271.64 não lida adequadamente com texturas, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-5123	O Skia, usado no Google Chrome antes de 23.0.1271.64, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2012-5122	O Google Chrome anterior a 23.0.1271.64 não executa adequadamente uma conversão de uma variável não especificada durante o processamento da entrada, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.
CVE-2012-5121	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.64 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao layout de vídeo.
CVE-2012-5120	O Google V8 anterior ao 3.13.7.5, conforme usado no Google Chrome antes de 23.0.1271.64, nas plataformas Linux de 64 bits permite que atacantes remotos causem uma negação de serviço ou

Nome	Descrição
	possivelmente tenham outro impacto não especificado por meio de código JavaScript criado que ative uma saída fora do limite acesso a um array.
CVE-2012-5119	A condição de corrida no Pepper, como usada no Google Chrome antes de 23.0.1271.64, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a buffers.
CVE-2012-5118	O Google Chrome anterior a 23.0.1271.64 no Mac OS X não valida corretamente um valor inteiro durante o tratamento dos buffers de comando da GPU, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-5117	O Google Chrome anterior a 23.0.1271.64 não restringe adequadamente o carregamento de uma sub-origem SVG no contexto de um elemento IMG, que possui vetores de impacto e ataque remoto não especificados.
CVE-2012-5116	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 23.0.1271.64 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de filtros SVG.
CVE-2012-5115	O Google Chrome anterior a 23.0.1271.64 no Mac OS X não atenua adequadamente o comportamento inadequado de gravação em drivers de gráficos, o que permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores desconhecidos que acionam "gravações desenfreadas".
CVE-2012-5112	A vulnerabilidade "usar-depois-livre" na implementação de SVG no WebKit, como usada no Google Chrome antes de 22.0.1229.94, permite que atacantes remotos executem código arbitrário por meio de vetores não especificados.
CVE-2012-5111	O Google Chrome anterior a 22.0.1229.92 não monitora falhas de plug-ins da Pepper, que possui vetores de impacto e ataque remoto não especificados.
CVE-2012-5110	O compositor no Google Chrome anterior a 22.0.1229.92 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2012-5109	A funcionalidade Componentes Internacionais para Unicode (ICU) no Google Chrome anterior a 22.0.1229.92 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores relacionados a uma expressão regular.
CVE-2012-5108	A condição de corrida no Google Chrome anterior a 22.0.1229.92 permite que atacantes remotos executem código arbitrário por meio de vetores relacionados a dispositivos de áudio.
CVE-2012-4930	O protocolo SPDY 3 e anterior, usado no Mozilla Firefox, no Google Chrome e em outros produtos, pode executar a criptografia TLS de

Nome	Descrição
	dados compactados sem ofuscar corretamente o tamanho dos dados não criptografados, o que permite que invasores intermediários obtenham texto simples Cabeçalhos HTTP observando as diferenças de comprimento durante uma série de suposições em que uma string em uma solicitação HTTP corresponde potencialmente a uma string desconhecida em um cabeçalho HTTP, também conhecido como ataque "CRIME".
CVE-2012-4929	O protocolo TLS 1.2 e anterior, usado no Mozilla Firefox, Google Chrome, Qt e outros produtos, pode criptografar dados compactados sem ofuscar adequadamente o tamanho dos dados não criptografados, o que permite que invasores man-in-the-middle obtenham HTTP em texto sem formatação. cabeçalhos observando as diferenças de comprimento durante uma série de suposições em que uma string em uma solicitação HTTP corresponde potencialmente a uma string desconhecida em um cabeçalho HTTP, também conhecido como ataque "CRIME".
CVE-2012-4909	O Google Chrome anterior a 18.0.1025308 no Android permite que atacantes remotos obtenham informações de cookies por meio de um aplicativo criado.
CVE-2012-4908	O Google Chrome anterior a 18.0.1025308 no Android permite que atacantes remotos contornem a Política de mesma origem e obtenham acesso a arquivos locais por meio de vetores que envolvam um link simbólico.
CVE-2012-4907	O Google Chrome anterior a 18.0.1025308 no Android não restringe adequadamente o acesso do código JavaScript às APIs do Android, o que permite que invasores remotos tenham um impacto não especificado por meio de uma página da Web criada.
CVE-2012-4906	O Google Chrome anterior a 18.0.1025308 no Android não restringe adequadamente o acesso ao arquivo: URLs, que permite que atacantes remotos obtenham informações confidenciais por meio de vetores não especificados, conforme demonstrado pela obtenção de dados de credenciais, uma vulnerabilidade diferente da CVE-2012-4903.
CVE-2012-4905	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome antes de 18.0.1025308 no Android permite que invasores remotos injetem script web arbitrário ou HTML por meio de um extra em um objeto Intent, também conhecido como "Universal XSS (UXSS)".
CVE-2012-4904	A vulnerabilidade de scripts entre aplicativos no Google Chrome anterior a 18.0.1025308 no Android permite que invasores remotos injetem scripts da web arbitrários por meio de vetores não especificados, conforme demonstrado pelos ataques "Universal XSS (UXSS)" na guia atual.
CVE-2012-4903	O Google Chrome anterior a 18.0.1025308 no Android não restringe adequadamente o acesso ao arquivo: URLs, que permite que atacantes remotos obtenham informações confidenciais por meio de vetores não especificados, conforme demonstrado pela obtenção de dados de credenciais, uma vulnerabilidade diferente

Nome	Descrição
	da CVE-2012-4906.
CVE-2012-4388	A função sapi_header_op no principal / SAPI.c no PHP 5.4.0RC2 a 5.4.0 não determina adequadamente um ponteiro durante verificações de sequências% 0D (caracteres de retorno de carro), o que permite que atacantes remotos contornem um mecanismo de proteção de divisão de resposta HTTP por meio de uma URL criada, relacionada à interação imprópria entre a função de cabeçalho do PHP e determinados navegadores, conforme demonstrado pelo Internet Explorer e pelo Google Chrome. NOTA: esta vulnerabilidade existe devido a uma correção incorreta para o CVE-2011-1398.
CVE-2012-4050	Várias vulnerabilidades não especificadas no Google Chrome OS anteriores a 21.0.1180.50 nas plataformas Cr-48 e Samsung Series 5 e 5 550 Chromebook e no Samsung Chromebox Series 3 têm impacto e vetores de ataque desconhecidos.
CVE-2012-3290	Várias vulnerabilidades não especificadas no Google Chrome antes de 20.0.1132.22 no Acer AC700; Samsung Series 5, 5 550 e Chromebox 3; e as plataformas Cr-48 do Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2012-2900	O Skia, usado no Google Chrome antes de 22.0.1229.92, não processa corretamente o texto, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente não tenham outro impacto por meio de vetores desconhecidos.
CVE-2012-2899	O Google Chrome anterior ao 21.0.1180.82 no iOS faz certas chamadas incorretas aos métodos WebView que acionam o uso de um applewebdata: URL, que permite que atacantes remotos contornem a Política de mesma origem e conduzam ataques de XSS universal (UXSS) por meio de vetores envolvendo o método document.write .
CVE-2012-2898	O Google Chrome anterior a 21.0.1180.82 no iOS em dispositivos iPad permite que invasores remotos falsifiquem o URL da Omnibox por meio de vetores envolvendo mensagens de erro SSL, um problema relacionado ao CVE-2012-0674.
CVE-2012-2897	Os drivers do modo kernel no Microsoft Windows XP SP2 e SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2 e R2 SP1, Windows 7 Gold e SP1, Windows 8, Windows Server 2012 e Windows RT, como usado pelo Google Chrome antes de 22.0.1229.79 e outros programas, não manipulam corretamente objetos na memória, o que permite que atacantes remotos executem código arbitrário por meio de um arquivo de fonte TrueType criado como "Vulnerabilidade de análise de fonte do Windows" ou "Vulnerabilidade de análise de fonte TrueType". "
CVE-2012-2896	O estouro de número inteiro na implementação do WebGL no Google Chrome antes de 22.0.1229.79 no Mac OS X permite que invasores remotos causem uma negação de serviço ou

Nome	Descrição
	possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2895	A funcionalidade PDF no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam operações de gravação fora dos limites.
CVE-2012-2894	O Google Chrome anterior a 22.0.1229.79 não lida adequadamente com estruturas de dados de contexto gráfico, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2893	A dupla vulnerabilidade livre na libxslt, como usada no Google Chrome antes de 22.0.1229.79, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a transformações XSL.
CVE-2012-2892	A vulnerabilidade não especificada no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos ignorem o bloqueador de pop-up por meio de vetores desconhecidos.
CVE-2012-2891	A implementação do IPC no Google Chrome antes de 22.0.1229.79 permite que os invasores obtenham informações potencialmente confidenciais sobre endereços de memória por meio de vetores não especificados.
CVE-2012-2890	A vulnerabilidade "usar-depois-de-livre" na funcionalidade do PDF no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2012-2889	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos injetem script web ou HTML arbitrário por meio de vetores que envolvam quadros, também conhecidos como "Universal XSS (UXSS)".
CVE-2012-2888	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 22.0.1229.79 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam referências de texto SVG.
CVE-2012-2887	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo eventos onclick.
CVE-2012-2886	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome anterior a 22.0.1229.79 permite que atacantes remotos injetem scripts da Web ou HTML arbitrários por meio de vetores relacionados às associações do Google V8, também conhecido como "XSS universal (UXSS)".
CVE-2012-2885	A dupla vulnerabilidade livre no Google Chrome anterior a

Nome	Descrição
CVE-2012-2884	22.0.1229.79 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à saída do aplicativo.
CVE-2012-2883	O Skia, usado no Google Chrome antes de 22.0.1229.79, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2012-2882	O Skia, usado no Google Chrome antes de 22.0.1229.79, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam uma operação de gravação fora dos limites, uma vulnerabilidade diferente da CVE-2012-2874.
CVE-2012-2881	O FFmpeg, como usado no Google Chrome antes de 22.0.1229.79, não manipula corretamente os contêineres OGG, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos, relacionados a um problema de "ponteiro selvagem".
CVE-2012-2880	A condição de corrida no Google Chrome anterior a 22.0.1229.79 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao buffer de tinta de plug-in.
CVE-2012-2879	O Google Chrome anterior a 22.0.1229.79 permite que invasores remotos causem uma negação de serviço (corrupção na árvore DOM) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2878	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de plug-in.
CVE-2012-2877	O sistema de extensão do Google Chrome anterior a 22.0.1229.79 não lida corretamente com diálogos modais, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2012-2876	O estouro de buffer na funcionalidade de otimização do SSE2 no Google Chrome anterior a 22.0.1229.79 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2875	Várias vulnerabilidades não especificadas na funcionalidade PDF no Google Chrome anteriores a 22.0.1229.79 permitem que invasores remotos tenham um impacto desconhecido por meio de um documento criado.

Nome	Descrição
CVE-2012-2874	O Skia, usado no Google Chrome antes de 22.0.1229.79, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam uma operação de gravação fora dos limites, uma vulnerabilidade diferente da CVE-2012-2883.
CVE-2012-2872	A vulnerabilidade de cross-site scripting (XSS) em uma página intersticial SSL no Google Chrome anterior a 21.0.1180.89 permite que invasores remotos injetem scripts da Web ou HTML arbitrários por meio de vetores não especificados.
CVE-2012-2871	A libxml2 2.9.0-rc1 e anterior, como usada no Google Chrome antes de 21.0.1180.89, não suporta adequadamente um elenco de uma variável não especificada durante o manuseio de transformações XSL, que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outros desconhecidos. impacto através de um documento elaborado, relacionado à estrutura de dados _xmlNs em include / libxml / tree.h.
CVE-2012-2870	A libxslt 1.1.26 e anterior, como usada no Google Chrome antes de 21.0.1180.89, não gerencia adequadamente a memória, o que pode permitir que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de uma expressão XSLT que não seja adequadamente identificada durante o XPath navegação, relacionada a (1) a função xsltCompileLocationPathPattern em libxslt / pattern.c e (2) a função xsltGenerateIdFunction em libxslt / functions.c.
CVE-2012-2869	O Google Chrome anterior a 21.0.1180.89 não carrega URLs corretamente, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam um "buffer obsoleto".
CVE-2012-2868	A condição de corrida no Google Chrome anterior a 21.0.1180.89 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo interação imprópria entre processos de trabalho e um objeto XMLHttpRequest (também conhecido como XHR).
CVE-2012-2867	A implementação do SPDY no Google Chrome anterior a 21.0.1180.89 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2012-2866	O Google Chrome anterior a 21.0.1180.89 não executa adequadamente um elenco de uma variável não especificada durante o tratamento de elementos de inicialização, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2012-2865	O Google Chrome anterior a 21.0.1180.89 não executa

Nome	Descrição
	corretamente a quebra de linha, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento criado.
CVE-2012-2864	O Mesa, usado no Google Chrome antes de 21.0.1183.0 nas plataformas Acer AC700, Cr-48 e Samsung Series 5 e 5 550 Chromebook e o Samsung Chromebox Series 3, permite que atacantes remotos executem código arbitrário por meio de vetores não especificados que açãoam um "estouro de matriz".
CVE-2012-2863	A funcionalidade PDF no Google Chrome anterior a 21.0.1180.75 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que açãoam operações de gravação fora dos limites.
CVE-2012-2862	A vulnerabilidade de uso após a liberação na funcionalidade PDF no Google Chrome anterior a 21.0.1180.75 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2012-2860	A implementação do selecionador de data no Google Chrome antes de 21.0.1180.57 no Mac OS X e Linux e antes de 21.0.1180.60 no Windows e no Chrome Frame permite que invasores remotos assistidos por usuário causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um site criado.
CVE-2012-2859	O Google Chrome anterior a 21.0.1180.57 no Linux não lida adequadamente com guias, o que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2012-2858	O estouro de buffer no decodificador WebP no Google Chrome antes de 21.0.1180.57 no Mac OS X e Linux e antes de 21.0.1180.60 no Windows e no Chrome Frame permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um WebP criado imagem.
CVE-2012-2857	A vulnerabilidade de uso após a atualização na implementação do DOM do Cascading Style Sheets (CSS) no Google Chrome antes de 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permite que atacantes remotos causem uma negação de serviço ou possivelmente não ter especificado outro impacto por meio de um documento criado.
CVE-2012-2856	A funcionalidade PDF no Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que são açãoados -bounds operações de gravação.
CVE-2012-2855	A vulnerabilidade de uso após a atualização da funcionalidade PDF no Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux e antes de 21.0.1180.60 no Windows e no Chrome Frame permite

Nome	Descrição
	que invasores remotos causem uma negação de serviço ou possivelmente outro impacto não especificado através de um documento elaborado.
CVE-2012-2854	O Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permite que atacantes remotos obtenham informações potencialmente confidenciais sobre valores de ponteiro, aproveitando o acesso a um processo de renderizador da WebUI.
CVE-2012-2853	A API webRequest no Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, não interage adequadamente com a Chrome Web Store, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente não especificou outro impacto através de um site criado.
CVE-2012-2852	A funcionalidade do PDF no Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux e antes de 21.0.1180.60 no Windows e no Chrome Frame não manipula adequadamente a vinculação de objetos, o que permite que atacantes remotos causem uma negação de serviço (use-after- gratuito) ou possivelmente não ter especificado outro impacto através de um documento elaborado.
CVE-2012-2851	Vários transbordamentos de números inteiros na funcionalidade PDF do Google Chrome anteriores a 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permitem que atacantes remotos causem uma negação de serviço ou possam ter outro impacto não especificado por meio de um trabalho documento.
CVE-2012-2850	Diversas vulnerabilidades não especificadas na funcionalidade PDF do Google Chrome anteriores a 21.0.1180.57 no Mac OS X e no Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permitem que invasores remotos tenham um impacto desconhecido por meio de um documento criado.
CVE-2012-2849	O erro "off-by-one" no decodificador GIF no Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permite que atacantes remotos causem uma negação de serviço (fora dos limites ler) através de uma imagem criada.
CVE-2012-2848	A implementação de arrastar e soltar no Google Chrome antes de 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, permite que atacantes remotos assistidos ignorem restrições de acesso a arquivos desejados por meio de um site criado.
CVE-2012-2847	O Google Chrome anterior a 21.0.1180.57 no Mac OS X e Linux, e antes de 21.0.1180.60 no Windows e no Chrome Frame, não solicita confirmação do usuário antes de continuar uma grande série de downloads, o que permite que invasores remotos assistidos causem uma negação de serviço (consumo de recursos)

Nome	Descrição
	através de um site criado.
CVE-2012-2846	O Google Chrome anterior a 21.0.1180.57 no Linux não isola adequadamente os processos do renderizador, o que permite que invasores remotos causem uma negação de serviço (interferência entre processos) por meio de vetores não especificados.
CVE-2012-2844	A funcionalidade do PDF no Google Chrome anterior a 20.0.1132.57 não processa adequadamente o código JavaScript, o que permite que invasores remotos causem uma negação de serviço (acesso incorreto a objetos) ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2012-2843	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.57 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao rastreamento de altura do layout.
CVE-2012-2842	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.57 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de contrapartida.
CVE-2012-2834	O estouro de número inteiro no Google Chrome anterior a 20.0.1132.43 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de dados criados no formato do contêiner Matroska.
CVE-2012-2833	O estouro de buffer na API JS na funcionalidade PDF no Google Chrome anterior a 20.0.1132.43 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2832	A implementação do codec de imagem na funcionalidade PDF no Google Chrome anterior a 20.0.1132.43 não inicializa um ponteiro não especificado, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2012-2831	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.43 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a referências de SVG.
CVE-2012-2830	O Google Chrome anterior a 20.0.1132.43 não define corretamente valores de matriz, o que permite que atacantes remotos causem uma negação de serviço (uso incorreto do ponteiro) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2829	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 20.0.1132.43 permite que atacantes remotos causem uma negação de serviço ou

Nome	Descrição
	tenham outro impacto não especificado por meio de vetores relacionados ao pseudoelemento: first-letter.
CVE-2012-2828	Vários transbordamentos de números inteiros na funcionalidade PDF no Google Chrome anteriores a 20.0.1132.43 permitem que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2012-2827	A vulnerabilidade de uso após a liberação na interface do usuário no Google Chrome antes de 20.0.1132.43 no Mac OS X permite que invasores causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2826	O Google Chrome anterior a 20.0.1132.43 não implementa adequadamente a conversão de texturas, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2012-2825	A implementação do XSL no Google Chrome antes de 20.0.1132.43 permite que atacantes remotos causem uma negação de serviço (operação de leitura incorreta) por meio de vetores não especificados.
CVE-2012-2824	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.43 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à pintura SVG.
CVE-2012-2823	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.43 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a recursos do SVG.
CVE-2012-2822	A funcionalidade PDF no Google Chrome anterior a 20.0.1132.43 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2012-2821	A implementação de preenchimento automático no Google Chrome anterior a 20.0.1132.43 não exibe corretamente o texto, que possui vetores de impacto e ataque remoto não especificados.
CVE-2012-2820	O Google Chrome anterior a 20.0.1132.43 não implementa corretamente filtros SVG, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2012-2819	A implementação de texSubImage2D no subsistema WebGL no Google Chrome antes de 20.0.1132.43 não manipula adequadamente carregamentos para texturas de ponto flutuante, o que permite que atacantes remotos causem uma negação de serviço (falha de declaração e falha de aplicativo) ou possivelmente tenham outro impacto não especificado por meio de um página web trabalhada, como demonstrado por alguns testes de desempenho WebGL, também conhecido como problema rdar

Nome	Descrição
11520387.	
CVE-2012-2818	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.43 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao layout de documentos que usam o recurso de contadores de CSS (Cascading Style Sheets).
CVE-2012-2817	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 20.0.1132.43 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a tabelas com seções.
CVE-2012-2816	O Google Chrome anterior a 20.0.1132.43 no Windows não isola adequadamente os processos em área restrita, o que pode permitir que invasores remotos causem uma negação de serviço (interferência de processo) por meio de vetores não especificados.
CVE-2012-2815	O Google Chrome anterior a 20.0.1132.43 permite que invasores remotos obtenham informações potencialmente confidenciais de um identificador de fragmento, aproveitando o acesso a um elemento IFRAME associado a um domínio diferente.
CVE-2012-2807	Vários overflows inteiros em libxml2, conforme usados no Google Chrome antes de 20.0.1132.43 e outros produtos, em plataformas Linux de 64 bits permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-2764	A vulnerabilidade do caminho de pesquisa não confiável no Google Chrome anterior a 20.0.1132.43 no Windows pode permitir que usuários locais obtenham privilégios por meio de uma DLL de metrô do cavalo de Tróia no diretório de trabalho atual.
CVE-2012-1846	O Google Chrome 17.0.963.66 e anteriores permitem que atacantes remotos contornem o mecanismo de proteção de sandbox, aproveitando o acesso a um processo de área restrita, conforme demonstrado pela VUPEN durante uma competição Pwn2Own na CanSecWest 2012. OBSERVAÇÃO: o principal produto afetado pode ser esclarecido posteriormente; Não foi identificado pelo pesquisador, que teria declarado "realmente não importa se é um código de terceiros".
CVE-2012-1845	A vulnerabilidade "usar-depois-livre" no Google Chrome 17.0.963.66 e anterior permite que atacantes remotos contornem os mecanismos de proteção DEP e ASLR e executem código arbitrário, por meio de vetores não especificados, conforme demonstrado pela VUPEN durante uma competição Pwn2Own no CanSecWest 2012. OBSERVAÇÃO: o produto primário afetado pode ser esclarecido posteriormente; Não foi identificado pelo pesquisador, que teria declarado que "realmente não importa se é um código de terceiros".
CVE-2012-1521	A vulnerabilidade "usar-depois-livre" no analisador XML no Google

Nome	Descrição
	Chrome antes de 18.0.1025.168 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2012-1418	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 17.0.963.60 nas plataformas Acer AC700, Samsung Series 5 e Cr-48 Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2012-1240	A vulnerabilidade de cross-site scripting (XSS) na extensão RECRUIT Dokodemo Rikunabi 2013 antes de 1.0.1 para o Google Chrome permite que atacantes remotos injetem script web arbitrário ou HTML através de vetores não especificados.
CVE-2012-0725	O Adobe Flash Player anterior a 11.2.202.229 no Google Chrome anterior a 18.0.1025.151 permite que os atacantes causem uma negação de serviço (corrupção de memória) ou, possivelmente, não tenham especificado outro impacto através de vetores desconhecidos, uma vulnerabilidade diferente da CVE-2012-0724.
CVE-2012-0724	O Adobe Flash Player anterior a 11.2.202.229 no Google Chrome anterior a 18.0.1025.151 permite que os atacantes causem uma negação de serviço (corrupção de memória) ou possam ter outro impacto não especificado através de vetores desconhecidos, uma vulnerabilidade diferente da CVE-2012-0725.
CVE-2012-0695	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 17.0.963.27 nas plataformas Acer AC700, Samsung Series 5 e Cr-48 Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2011-5319	content / renderer / device_sensors / device_motion_event_pump.cc no Google Chrome anterior a 41.0.2272.76 não restringe adequadamente o acesso a dados de acelerômetro de alta taxa, o que facilita para invasores remotos capturar pressionamentos de teclas por meio de um site criado para ouvir eventos de emoção, vulnerabilidade diferente de CVE-2015-1231.
CVE-2011-4719	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 16.0.912.63 nas plataformas Acer AC700, Samsung Series 5 e Cr-48 Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2011-4692	O WebKit, como usado no Apple Safari 5.1.1 e anteriores e no Google Chrome 15 e anteriores, não impede a captura de dados sobre o tempo necessário para o carregamento de imagens, o que facilita para invasores remotos determinar se existe uma imagem no cache do navegador via código JavaScript criado, conforme demonstrado por visipisi.
CVE-2011-4691	O Google Chrome 15.0.874.121 e anteriores não impedem a captura de dados sobre os tempos de violações de Política de Origem Mesmo durante as tentativas de carregamento do IFRAME, o que facilita para os invasores remotos determinar se existe um documento no cache do navegador por meio de código JavaScript

Nome	Descrição
	criado.
CVE-2011-4548	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 16.0.912.44 nas plataformas Acer AC700, Samsung Series 5 e Cr-48 Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2011-3972	A implementação do tradutor de sombreador no Google Chrome anterior a 17.0.963.46 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3971	A vulnerabilidade "usar-depois-de-graça" no Google Chrome anterior a 17.0.963.46 permite que invasores remotos assistidos por usuários causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a eventos do mousemove.
CVE-2011-3970	A libxslt, como usada no Google Chrome antes de 17.0.963.46, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3969	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.46 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao layout de documentos SVG.
CVE-2011-3968	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.46 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem sequências de tokens de CSS (Cascading Style Sheets).
CVE-2011-3967	A vulnerabilidade não especificada no Google Chrome anterior a 17.0.963.46 permite que invasores remotos causem uma negação de serviço (falha do aplicativo) por meio de um certificado criado.
CVE-2011-3966	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.46 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de erros para dados de sequência de token em cascata (CSS).
CVE-2011-3965	O Google Chrome anterior a 17.0.963.46 não verifica corretamente as assinaturas, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2011-3964	O Google Chrome anterior a 17.0.963.46 não implementa adequadamente o recurso de arrastar e soltar, o que facilita para invasores remotos falsificar a barra de URL por meio de vetores não especificados.
CVE-2011-3963	O Google Chrome anterior a 17.0.963.46 não processa adequadamente imagens PDF FAX, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites)

Nome	Descrição
	por meio de vetores não especificados.
CVE-2011-3962	O Google Chrome anterior a 17.0.963.46 não executa corretamente o recorte de caminho, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3961	A condição de corrida no Google Chrome anterior a 17.0.963.46 permite que atacantes remotos executem código arbitrário por meio de vetores que acionam uma falha de um processo de utilitário.
CVE-2011-3960	O Google Chrome anterior a 17.0.963.46 não decodifica corretamente os dados de áudio, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3959	O estouro de buffer na implementação de local no Google Chrome anterior a 17.0.963.46 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3958	O Google Chrome anterior a 17.0.963.46 não executa corretamente conjuntos de variáveis durante o tratamento de um período de coluna, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2011-3957	A vulnerabilidade "usar-depois-livre" na funcionalidade de coleta de lixo do Google Chrome anterior a 17.0.963.46 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo documentos PDF.
CVE-2011-3956	A implementação da extensão no Google Chrome anterior a 17.0.963.46 não lida corretamente com origens de sandbox, o que pode permitir que atacantes remotos contornem a Política de mesma origem por meio de uma extensão criada.
CVE-2011-3955	O Google Chrome anterior a 17.0.963.46 permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou, possivelmente, não tenham especificado outro impacto por meio de vetores que acionam o aborto de uma transação do IndexedDB.
CVE-2011-3954	O Google Chrome anterior a 17.0.963.46 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores que acionam uma grande quantidade de uso do banco de dados.
CVE-2011-3953	O Google Chrome anterior a 17.0.963.46 não impede o monitoramento da área de transferência após um evento de colagem, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-3928	A vulnerabilidade de uso após a liberação no Google Chrome antes de 16.0.912.77 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificados.

Nome	Descrição
CVE-2011-3927	especificado por meio de vetores relacionados ao manuseio do DOM.
CVE-2011-3926	O Skia, como usado no Google Chrome antes de 16.0.912.77, não executa toda a inicialização necessária de valores, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3925	O estouro de buffer com base em heap no criador de árvores no Google Chrome anterior a 16.0.912.77 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3924	A vulnerabilidade de uso após a liberação no recurso de Navegação segura no Google Chrome antes de 16.0.912.75 permite que invasores remotos causem uma negação de serviço (corrupção de memória de heap) ou possivelmente outro impacto não especificado por meio de vetores relacionados a uma entrada de navegação e uma página intersticial.
CVE-2011-3922	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 16.0.912.77 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a seleções DOM.
CVE-2011-3921	O estouro de buffer baseado em pilha no Google Chrome antes de 16.0.912.75 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de glifos.
CVE-2011-3919	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 16.0.912.75 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo quadros de animação.
CVE-2011-3917	O estouro de buffer com base em heap na libxml2, conforme usado no Google Chrome antes de 16.0.912.75, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3916	O estouro de buffer baseado em pilha no FileWatcher no Google Chrome antes de 16.0.912.63 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3915	O Google Chrome anterior a 16.0.912.63 não processa corretamente referências cruzadas de PDF, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3915	O estouro de buffer no Google Chrome anterior a 16.0.912.63 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a fontes PDF.

Nome	Descrição
CVE-2011-3914	A funcionalidade de internacionalização (i18n) no Google V8, usada no Google Chrome antes de 16.0.912.63, permite que atacantes remotos causem uma negação de serviço ou possivelmente não tenham outro impacto por meio de vetores desconhecidos que acionam uma gravação fora dos limites.
CVE-2011-3913	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 16.0.912.63 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento do intervalo.
CVE-2011-3912	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 16.0.912.63 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a filtros SVG.
CVE-2011-3911	O Google Chrome anterior a 16.0.912.63 não processa adequadamente documentos PDF, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3910	O Google Chrome anterior a 16.0.912.63 não processa adequadamente frames de vídeo YUV, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3909	A implementação de CSS (Cascading Style Sheets) no Google Chrome anterior a 16.0.912.63 em plataformas de 64 bits não gerencia adequadamente matrizes de propriedade, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados.
CVE-2011-3908	O Google Chrome anterior a 16.0.912.63 não analisa corretamente documentos SVG, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3907	O recurso de fonte de visualização do Google Chrome anterior a 16.0.912.63 permite que invasores remotos falsifiquem a barra de URL por meio de vetores não especificados.
CVE-2011-3906	O analisador de PDF no Google Chrome anterior a 16.0.912.63 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3905	A libxml2, conforme usada no Google Chrome antes de 16.0.912.63, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3904	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 16.0.912.63 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de texto bidirecional (também conhecido como bidi).

Nome	Descrição
CVE-2011-3903	O Google Chrome anterior a 16.0.912.63 não executa corretamente correspondência de regex, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3900	O Google V8, usado no Google Chrome antes de 15.0.874.121, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que acionam uma operação de gravação fora dos limites.
CVE-2011-3898	O Google Chrome antes de 15.0.874.120, quando o Java Runtime Environment (JRE) 7 é usado, não solicita confirmação do usuário antes do início da execução do applet, o que permite que invasores remotos tenham um impacto não especificado por meio de um applet criado.
CVE-2011-3897	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 15.0.874.120 permite que invasores remotos assistidos por usuários causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à edição.
CVE-2011-3896	O estouro de buffer no Google Chrome anterior a 15.0.874.120 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao mapeamento de variáveis de shader.
CVE-2011-3895	O estouro de buffer com base em heap no decodificador Vorbis no Google Chrome antes de 15.0.874.120 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um fluxo criado.
CVE-2011-3894	O Google Chrome anterior a 15.0.874.120 não executa corretamente a decodificação do VP8, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de um fluxo criado.
CVE-2011-3893	O Google Chrome anterior a 15.0.874.120 não implementa adequadamente os manipuladores de mídia MKV e Vorbis, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3892	A dupla vulnerabilidade livre no decodificador Theora no Google Chrome antes de 15.0.874.120 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um fluxo criado.
CVE-2011-3891	O Google Chrome anterior a 15.0.874.102 não restringe adequadamente o acesso a funções internas do Google V8, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3890	A vulnerabilidade de uso após a liberação no Google Chrome antes de 15.0.874.102 permite que invasores remotos causem uma

Nome	Descrição
	negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento da origem de vídeo.
CVE-2011-3889	O estouro de buffer baseado em heap na implementação do Web Audio no Google Chrome antes de 15.0.874.102 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3888	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 15.0.874.102 permite que invasores remotos assistidos por usuário causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a operações de edição em conjunto com um plug-in desconhecido.
CVE-2011-3887	O Google Chrome anterior a 15.0.874.102 não manipula corretamente o javascript: URLs, que permite que atacantes remotos contornem as restrições de acesso pretendidas e leiam cookies por meio de vetores não especificados.
CVE-2011-3886	O Google V8, conforme usado no Google Chrome antes de 15.0.874.102, permite que atacantes remotos causem uma negação de serviço ou possivelmente não tenham outro impacto específico por meio de códigos JavaScript criados que acionam operações de gravação fora dos limites.
CVE-2011-3885	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 15.0.874.102 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a dados sequenciais de token em cascata do CSS (Cascading Style Sheets).
CVE-2011-3884	O Google Chrome anterior a 15.0.874.102 não corrige problemas de tempo durante a passagem de DOM, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2011-3883	A vulnerabilidade de uso após a liberação no Google Chrome antes de 15.0.874.102 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a contadores.
CVE-2011-3882	A vulnerabilidade de uso após a liberação no Google Chrome antes de 15.0.874.102 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a buffers de mídia.
CVE-2011-3881	O WebKit, usado no Google Chrome antes de 15.0.874.102 e Android antes do 4.4, permite que atacantes remotos contornem a Política de mesma origem e conduzam ataques de XSS universal (UXSS) através de vetores relacionados a (1) a função DOMWindow :: clear e uso de um objeto de seleção, (2) a função Object :: GetRealNamedPropertyInPrototypeChain e uso de uma

Nome	Descrição
CVE-2011-3880	propriedade __proto__, (3) a função HTMLPlugInImageElement :: allowedToLoadFrameURL e uso de uma origem javascript: URL, (4) incorreta para documentos gerados por XSLT no XSLTProcessor: : função createDocumentFromSource e (5) manuseio inadequado de cargas de quadros síncronos na função ScriptController :: executeIfJavaScriptURL.
CVE-2011-3879	O Google Chrome anterior a 15.0.874.102 não impede o uso de um caractere especial não especificado como um delimitador nos cabeçalhos HTTP, que tem impacto desconhecido e vetores de ataque remoto.
CVE-2011-3878	O Google Chrome anterior a 15.0.874.102 não impede o redirecionamento para o chrome: URLs, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-3877	A condição de corrida no Google Chrome anterior a 15.0.874.102 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à inicialização do processo de trabalho.
CVE-2011-3876	A vulnerabilidade de script entre sites (XSS) na página de internalização do appcache no Google Chrome antes de 15.0.874.102 permite que atacantes remotos injetem script da Web ou HTML arbitrário por meio de vetores não especificados.
CVE-2011-3875	O Google Chrome anterior a 15.0.874.102 não processa adequadamente o download de arquivos que possuem caracteres de espaço em branco no final de um nome de arquivo, que possui vetores de impacto remoto não especificado e ataque assistido pelo usuário.
CVE-2011-3873	O Google Chrome anterior a 15.0.874.102 não lida corretamente com operações de arrastar e soltar em cadeias de URL, o que permite que invasores remotos assistidos por usuário falsifiquem a barra de URL por meio de vetores não especificados.
CVE-2011-3640	** DISPUTADO ** Vulnerabilidade de caminho de pesquisa não confiável no Mozilla Network Security Services (NSS), usado no Google Chrome antes de 17 no Windows e Mac OS X, pode permitir que usuários locais obtenham privilégios através de um arquivo de cavalo de tróia pkcs11.txt diretório de nível. OBSERVAÇÃO: a resposta do fornecedor foi "Comportamento estranho, mas não estamos tratando isso como um bug de segurança".
CVE-2011-3421	Várias vulnerabilidades não especificadas no Google Chrome anteriores a 14.0.835.125 nas plataformas Acer AC700, Samsung Series 5 e Cr-48 Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2011-3420	Várias vulnerabilidades não especificadas no Google Chrome

Nome	Descrição
	anteriores a 14.0.835.157 nas plataformas Acer AC700, Samsung Series 5 e Cr-48 Chromebook têm impacto e vetores de ataque desconhecidos.
CVE-2011-3389	O protocolo SSL, usado em certas configurações no Microsoft Windows e no Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera e outros produtos, criptografa os dados usando o modo CBC com vetores de inicialização encadeados, o que permite que os invasores man-in-the-middle obter cabeçalhos HTTP de texto sem formatação por meio de um blockwise boundary attack (BCBA) em uma sessão HTTPS, em conjunto com o código JavaScript que usa (1) a API WebSocket HTML5, (2) a API Java URLConnection ou (3) o WebClient Silverlight API, também conhecido como ataque "BEAST".
CVE-2011-3234	O Google Chrome anterior a 14.0.835.163 não manipula corretamente caixas, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3115	O Google V8, conforme usado no Google Chrome antes de 19.0.1084.52, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam a "corrupção de tipos".
CVE-2011-3114	Vários buffer overflows na funcionalidade PDF no Google Chrome anteriores a 19.0.1084.52 permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam chamadas de função desconhecidas.
CVE-2011-3113	A funcionalidade do PDF no Google Chrome anterior a 19.0.1084.52 não executa adequadamente uma conversão de uma variável não especificada durante o manuseio de espaços de cores, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2011-3112	A vulnerabilidade "usar-depois-de-livre" na funcionalidade PDF no Google Chrome anterior a 19.0.1084.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criptografado inválido.
CVE-2011-3111	O Google V8, usado no Google Chrome antes de 19.0.1084.52, permite que invasores remotos causem uma negação de serviço (operação de leitura inválida) por meio de vetores não especificados.
CVE-2011-3110	A funcionalidade PDF no Google Chrome anterior a 19.0.1084.52 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que acionam operações de gravação fora dos limites.
CVE-2011-3109	O Google Chrome anterior a 19.0.1084.52 no Linux não executa

Nome	Descrição
CVE-2011-3108	adequadamente uma conversão de uma variável não especificada, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido, aproveitando um erro na implementação da interface do usuário do GTK.
CVE-2011-3107	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 19.0.1084.52 permite que atacantes remotos executem código arbitrário por meio de vetores relacionados ao cache do navegador.
CVE-2011-3106	O Google Chrome anterior a 19.0.1084.52 não implementa corretamente as vinculações de JavaScript para plug-ins, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3105	A implementação de WebSockets no Google Chrome anterior a 19.0.1084.52 não lida adequadamente com o uso de SSL, que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados.
CVE-2011-3104	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 19.0.1084.52 permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados ao pseudoelemento de primeira letra.
CVE-2011-3103	O Skia, como usado no Google Chrome antes de 19.0.1084.52, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3102	O Google V8, usado no Google Chrome antes de 19.0.1084.52, não executa corretamente a coleta de lixo, o que permite que atacantes remotos causem uma negação de serviço (falha no aplicativo) ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado.
CVE-2011-3101	O erro "off-by-one" na libxml2, usado no Google Chrome antes de 19.0.1084.46 e outros produtos, permite que atacantes remotos causem uma negação de serviço (gravação fora do limite) ou possivelmente não tenham outro impacto por meio de vetores desconhecidos.
CVE-2011-3100	O Google Chrome anterior a 19.0.1084.46 no Linux não atenua adequadamente uma falha não especificada em um driver NVIDIA, que tem impacto e vetores de ataque desconhecidos. NOTA: consulte CVE-2012-3105 para o problema relacionado ao MFSA 2012-34 nos produtos Mozilla.
CVE-2011-3099	A vulnerabilidade "usar-depois-livre" na funcionalidade PDF do

Nome	Descrição
	Google Chrome anterior a 19.0.1084.46 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam um nome malformado para a codificação de fonte.
CVE-2011-3098	O Google Chrome anterior a 19.0.1084.46 no Windows usa um caminho de pesquisa incorreto para o plug-in do Windows Media Player, o que pode permitir que usuários locais obtenham privilégios por meio de um plug-in de cavalo de Tróia em um diretório não especificado.
CVE-2011-3097	A funcionalidade PDF no Google Chrome anterior a 19.0.1084.46 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando um erro de gravação fora dos limites na implementação de funções de amostra.
CVE-2011-3096	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 19.0.1084.46 no Linux permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado, aproveitando um erro na implementação da GTN na omnibox.
CVE-2011-3095	O contêiner OGG no Google Chrome anterior a 19.0.1084.46 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que acionam uma gravação fora dos limites.
CVE-2011-3094	O Google Chrome anterior a 19.0.1084.46 não processa adequadamente o texto tibetano, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3093	O Google Chrome anterior a 19.0.1084.46 não manipula corretamente os glifos, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3092	A implementação da regex no Google V8, conforme usada no Google Chrome antes de 19.0.1084.46, permite que invasores remotos causem uma negação de serviço (operação de gravação inválida) ou possivelmente não tenham outro impacto desconhecido por meio de vetores desconhecidos.
CVE-2011-3091	A vulnerabilidade "use-after-free" na implementação do IndexedDB no Google Chrome antes de 19.0.1084.46 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3090	A condição de corrida no Google Chrome anterior a 19.0.1084.46 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a processos de trabalho.
CVE-2011-3089	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 19.0.1084.46 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto

Nome	Descrição
	não especificado por meio de vetores envolvendo tabelas.
CVE-2011-3088	O Google Chrome anterior a 19.0.1084.46 não desenha adequadamente as linhas aéreas, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3087	O Google Chrome anterior a 19.0.1084.46 não realiza corretamente a navegação na janela, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-3086	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 19.0.1084.46 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam um elemento STYLE.
CVE-2011-3085	O recurso de preenchimento automático no Google Chrome anterior a 19.0.1084.46 não restringe adequadamente os valores de campo, o que permite que invasores remotos causem uma negação de serviço (corrupção da interface do usuário) e possivelmente realizem ataques de falsificação por meio de vetores envolvendo valores longos.
CVE-2011-3084	O Google Chrome anterior a 19.0.1084.46 não utiliza um processo dedicado para o carregamento de links encontrados em uma página interna, o que pode permitir que invasores ignorem restrições de sandbox pretendidas por meio de uma página criada.
CVE-2011-3083	browser / profiles / profile_impl_io_data.cc no Google Chrome anterior a 19.0.1084.46 não manipula corretamente uma URL ftp malformada no atributo SRC de um elemento VIDEO, que permite que atacantes remotos causem uma negação de serviço (desreferenciamento de ponteiro NULL e falha de aplicativo) uma página da web trabalhada.
CVE-2011-3081	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.168 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à flutuação de elementos, uma vulnerabilidade diferente da CVE-2011-3078.
CVE-2011-3080	A condição de corrida na implementação da comunicação entre processos (IPC) no Google Chrome antes de 18.0.1025.168 permite que os atacantes contornem restrições de sandbox pretendidas através de vetores não especificados.
CVE-2011-3079	A implementação da comunicação entre processos (IPC) no Google Chrome antes de 18.0.1025.168, conforme usada no Mozilla Firefox antes de 38.0 e outros produtos, não valida corretamente as mensagens, que têm impacto não especificado e vetores de ataque.
CVE-2011-3078	A vulnerabilidade "usar-depois-de-graça" no Google Chrome anterior a 18.0.1025.168 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à flutuação de

Nome	Descrição
	elementos, uma vulnerabilidade diferente da CVE-2011-3081.
CVE-2011-3077	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo as ligações de script, relacionadas a um problema de "leitura livre".
CVE-2011-3076	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de foco.
CVE-2011-3075	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a comandos de estilo de aplicativo.
CVE-2011-3074	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de mídia.
CVE-2011-3073	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de recursos SVG.
CVE-2011-3072	O Google Chrome anterior a 18.0.1025.151 permite que invasores remotos ignorem a Política de mesma origem por meio de vetores relacionados a janelas pop-up.
CVE-2011-3071	A vulnerabilidade de uso após a liberação na implementação de HTMLMediaElement no Google Chrome antes de 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3070	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.151 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados às associações do Google V8.
CVE-2011-3069	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 18.0.1025.151 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a caixas de linha.
CVE-2011-3068	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 18.0.1025.151 permite que atacantes remotos causem uma

Nome	Descrição
	negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados a caixas de entrada.
CVE-2011-3067	O Google Chrome anterior a 18.0.1025.151 permite que invasores remotos ignorem a Política de mesma origem por meio de vetores relacionados à substituição de elementos IFRAVE.
CVE-2011-3066	O Skia, como usado no Google Chrome antes de 18.0.1025.151, não executa corretamente o recorte, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3065	O Skia, como usado no Google Chrome antes de 18.0.1025.142, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3064	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 18.0.1025.142 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao recorte de SVG.
CVE-2011-3063	O Google Chrome anterior a 18.0.1025.142 não valida corretamente as solicitações de navegação do renderizador, que têm vetores de impacto e ataque remoto não especificados.
CVE-2011-3062	O erro "off-by-one" no OpenType Sanitizer no Google Chrome anterior a 18.0.1025.142 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um arquivo OpenType criado.
CVE-2011-3061	O Google Chrome anterior a 18.0.1025.142 não verifica adequadamente os certificados X.509 antes de usar um proxy SPDY, o que pode permitir que invasores intermediários falsifiquem servidores ou obtenham informações confidenciais por meio de um certificado criado.
CVE-2011-3060	O Google Chrome anterior a 18.0.1025.142 não lida adequadamente com fragmentos de texto, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3059	O Google Chrome anterior a 18.0.1025.142 não processa adequadamente elementos de texto SVG, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3058	O Google Chrome anterior a 18.0.1025.142 não lida corretamente com o sistema de codificação EUC-JP, o que pode permitir que atacantes remotos realizem ataques XSS (cross-site scripting) por meio de vetores não especificados.
CVE-2011-3057	O Google V8, usado no Google Chrome antes de 17.0.963.83, permite que atacantes remotos causem uma negação de serviço por meio de vetores que acionam uma operação de leitura inválida.
CVE-2011-3056	O Google Chrome anterior a 17.0.963.83 permite que invasores

Nome	Descrição
	remotos ignorem a Política de mesma origem por meio de vetores que envolvam um "iframe mágico".
CVE-2011-3055	A interface do usuário nativa do navegador no Google Chrome anterior a 17.0.963.83 não exige confirmação do usuário antes de uma instalação de extensão descompactada, o que permite que invasores remotos assistidos pelo usuário tenham um impacto não especificado por meio de uma extensão criada.
CVE-2011-3054	A implementação de privilégios da WebUI no Google Chrome anterior a 17.0.963.83 não realiza corretamente o isolamento, o que permite que atacantes remotos contornem as restrições de acesso pretendidas por meio de vetores não especificados.
CVE-2011-3053	A vulnerabilidade "usar-depois-de-graça" no Google Chrome anterior a 17.0.963.83 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à divisão de blocos.
CVE-2011-3052	A implementação de WebGL no Google Chrome anterior a 17.0.963.83 não manipula adequadamente os elementos de CANVAS, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3051	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 17.0.963.83 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à função de cross-fade.
CVE-2011-3050	A vulnerabilidade "usar-depois-livre" na implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 17.0.963.83 permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores relacionados ao pseudoelemento de primeira letra.
CVE-2011-3049	O Google Chrome anterior a 17.0.963.83 não restringe adequadamente a API de solicitação da Web de extensão, o que permite que invasores remotos causem uma negação de serviço (solicitações de sistema interrompidas) por meio de uma extensão criada.
CVE-2011-3047	O processo de GPU no Google Chrome anterior a 17.0.963.79 permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória), aproveitando um erro no mecanismo de carregamento de plug-ins.
CVE-2011-3046	O subsistema de extensão no Google Chrome anterior a 17.0.963.78 não lida corretamente com a navegação de histórico, o que permite que atacantes remotos executem códigos arbitrários aproveitando um problema de "XSS universal (UXSS)".
CVE-2011-3045	Erro de assinatura de número inteiro na função png_inflate em pngrutil.c na libpng anterior a 1.4.10beta01, usado no Google

Nome	Descrição
CVE-2011-3044	Chrome antes de 17.0.963.83 e outros produtos, permite que atacantes remotos causem uma negação de serviço (falha de aplicativo) ou possivelmente executar código arbitrário via um arquivo PNG criado, uma vulnerabilidade diferente da CVE-2011-3026.
CVE-2011-3043	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.65 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem elementos de animação SVG.
CVE-2011-3042	A vulnerabilidade "usar-depois-livre" no Google Chrome anterior a 17.0.963.65 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo um flexbox (também conhecido como caixa flexível) em conjunto com elementos flutuantes.
CVE-2011-3041	A vulnerabilidade "usar-depois-de-graça" no Google Chrome anterior a 17.0.963.65 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio das seções da tabela.
CVE-2011-3040	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.65 permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento criado.
CVE-2011-3039	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.65 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de cotação.
CVE-2011-3038	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.65 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de várias colunas.
CVE-2011-3037	O Google Chrome anterior a 17.0.963.65 não executa corretamente conjuntos de variáveis não especificadas durante a divisão de blocos anônimos, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2011-3036	O Google Chrome anterior a 17.0.963.65 não executa adequadamente uma conversão de uma variável não especificada

Nome	Descrição
	durante o processamento de caixas de linha, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2011-3035	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.65 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem elementos de uso do SVG.
CVE-2011-3034	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.65 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo um documento SVG.
CVE-2011-3033	O estouro de buffer no Skia, conforme usado no Google Chrome antes de 17.0.963.65, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3032	A vulnerabilidade "usar-depois-de-graça" no Google Chrome anterior a 17.0.963.65 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de valores SVG.
CVE-2011-3031	A vulnerabilidade "usar após liberar" no wrapper do elemento no Google V8, conforme usada no Google Chrome antes de 17.0.963.65, permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-3027	O Google Chrome anterior a 17.0.963.56 não executa adequadamente uma conversão de uma variável não especificada durante o processamento de colunas, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2011-3026	O estouro de inteiro na libpng, como usado no Google Chrome antes de 17.0.963.56, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que açãoam um truncamento de números inteiros.
CVE-2011-3025	O Google Chrome anterior a 17.0.963.56 não analisa adequadamente os dados H.264, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-3024	O Google Chrome anterior a 17.0.963.56 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de um certificado X.509 vazio.
CVE-2011-3023	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.56 permite que invasores remotos assistidos

Nome	Descrição
	por usuário causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a operações de arrastar e soltar.
CVE-2011-3022	traduza / translate_manager.cc no Google Chrome antes de 17.0.963.56 e 19.x antes de 19.0.1036.7 usa uma sessão HTTP para trocar dados por tradução, o que permite que atacantes remotos obtenham informações confidenciais cheirando a rede.
CVE-2011-3021	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.56 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao carregamento de subquadro.
CVE-2011-3020	A vulnerabilidade não especificada na implementação do validador do Native Client no Google Chrome anterior a 17.0.963.56 tem vetores de impacto e ataque remoto desconhecidos.
CVE-2011-3019	O estouro de buffer com base em heap no Google Chrome anterior a 17.0.963.56 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um arquivo de vídeo Matroska (também conhecido como MKV).
CVE-2011-3018	O estouro de buffer com base em heap no Google Chrome anterior a 17.0.963.56 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à renderização de caminho.
CVE-2011-3017	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 17.0.963.56 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de banco de dados.
CVE-2011-3016	A vulnerabilidade de uso após liberação no Google Chrome anterior a 17.0.963.56 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo nós de contadores, relacionados a um problema de "leitura livre".
CVE-2011-3015	Vários overflows inteiros nos codecs PDF no Google Chrome anteriores a 17.0.963.56 permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2881	O Google Chrome anterior a 14.0.835.202 não manipula corretamente os objetos ocultos do Google V8, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de código JavaScript criado.
CVE-2011-2880	A vulnerabilidade de uso após a liberação no Google Chrome antes de 14.0.835.202 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não

Nome	Descrição
	especificado por meio de vetores relacionados às associações do Google V8.
CVE-2011-2879	O Google Chrome anterior a 14.0835.202 não considera adequadamente a vida útil do objeto e a segurança do thread durante o manuseio de nós de áudio, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2878	O Google Chrome anterior a 14.0835.202 não restringe adequadamente o acesso ao protótipo de janela, o que permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2011-2877	O Google Chrome anterior a 14.0835.202 não processa corretamente o texto SVG, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "fonte obsoleta".
CVE-2011-2876	A vulnerabilidade de uso após a liberação no Google Chrome antes de 14.0835.202 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvam uma caixa de linha de texto.
CVE-2011-2875	O Google V8, usado no Google Chrome antes de 14.0835.163, não realiza corretamente o selamento de objetos, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que geram "confusão de tipo".
CVE-2011-2874	O Google Chrome anterior a 14.0.835.163 não realiza uma operação de pin esperada para um certificado autoassinado durante uma sessão, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-2864	O Google Chrome anterior a 14.0.835.163 não lida corretamente com caracteres tibetanos, o que permite que invasores remotos causem uma negação de serviço (leituras fora dos limites) por meio de vetores não especificados.
CVE-2011-2862	O Google V8, usado no Google Chrome antes de 14.0835.163, não restringe adequadamente o acesso a objetos internos, que têm vetores de impacto e ataque remoto não especificados.
CVE-2011-2861	O Google Chrome anterior a 14.0.835.163 não lida corretamente com strings em documentos PDF, o que permite que invasores remotos tenham um impacto não especificado por meio de um documento criado que aciona uma operação de leitura incorreta.
CVE-2011-2860	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 14.0.835.163 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a estilos de tabela.

Nome	Descrição
CVE-2011-2859	O Google Chrome anterior a 14.0.835.163 usa permissões incorretas para páginas que não são de galeria, o que tem impacto não especificado e vetores de ataque.
CVE-2011-2858	O Google Chrome anterior a 14.0.835.163 não lida corretamente com arrays triangulares, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2857	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 14.0.835.163 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao controlador de foco.
CVE-2011-2856	O Google V8, conforme usado no Google Chrome antes de 14.0.835.163, permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2011-2855	O Google Chrome anterior a 14.0.835.163 não processa adequadamente as seqüências de tokens do Cascading Style Sheets (CSS), o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "nó obsoleto".
CVE-2011-2854	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 14.0.835.163 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a "entrega em estilo ruby / table".
CVE-2011-2853	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 14.0.835.163 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio de plug-in.
CVE-2011-2852	O erro "off-by-one" no Google V8, usado no Google Chrome antes de 14.0.835.163, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2851	O Google Chrome anterior a 14.0.835.163 não lida corretamente com vídeo, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2850	O Google Chrome anterior a 14.0.835.163 não manipula corretamente caracteres Khmer, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2849	A implementação de WebSockets no Google Chrome antes de 14.0.835.163 permite que invasores remotos causem uma negação de serviço (desreferenciamento de ponteiro NULL e falha de aplicativo) por meio de vetores não especificados.

Nome	Descrição
CVE-2011-2848	O Google Chrome anterior a 14.0.835.163 permite que invasores remotos assistidos por usuários falsifiquem a barra de URL por meio de vetores relacionados ao botão de encaminhamento.
CVE-2011-2847	A vulnerabilidade "usar-depois-livre" no carregador de documentos do Google Chrome anterior a 14.0.835.163 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2011-2846	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 14.0.835.163 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de eventos de descarregamento.
CVE-2011-2845	O Google Chrome anterior a 15.0.874.102 não processa corretamente os dados do histórico, o que permite que invasores remotos assistidos por usuário falsifiquem a barra de URL por meio de vetores não especificados.
CVE-2011-2844	O Google Chrome anterior a 14.0.835.163 não processa corretamente arquivos MP3, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2843	O Google Chrome anterior a 14.0.835.163 não lida adequadamente com buffers de mídia, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2842	O instalador no Google Chrome anterior a 14.0.835.163 no Mac OS X não lida adequadamente com arquivos de bloqueio, que têm vetores de impacto e de ataque não especificados.
CVE-2011-2841	O Google Chrome anterior a 14.0.835.163 não executa corretamente a coleta de lixo durante o processamento de documentos PDF, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2011-2840	O Google Chrome anterior a 14.0.835.163 permite que invasores remotos assistidos por usuários falsifiquem a barra de URL por meio de vetores relacionados a "interação incomum com o usuário".
CVE-2011-2839	A implementação do PDF no Google Chrome antes de 13.0.782.215 no Linux não usa corretamente a função de biblioteca memset, que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2838	O Google Chrome anterior a 14.0.835.163 não considera adequadamente o tipo MIME durante o carregamento de um plug-in, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-2837	O Google Chrome anterior a 14.0.835.163 no Linux não usa as

Nome	Descrição
	opções de compilador PIC e PIE para código independente de posição, que possui vetores de impacto e de ataque não especificados.
CVE-2011-2836	O Google Chrome anterior a 14.0.835.163 não exige interação com o Infobar antes do uso do plug-in do Windows Media Player, o que facilita para que invasores remotos tenham um impacto não especificado por meio de conteúdo Flash criado.
CVE-2011-2835	A condição de corrida no Google Chrome anterior a 14.0.835.163 permite que invasores causem uma negação de serviço ou possivelmente não tenham outro impacto específico por meio de vetores relacionados ao cache de certificado.
CVE-2011-2834	A dupla vulnerabilidade livre na libxml2, conforme usada no Google Chrome antes de 14.0.835.163, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de XPath.
CVE-2011-2830	O Google V8, usado no Google Chrome antes de 14.0835.163, não implementa adequadamente os wrappers de objeto de script, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2829	O estouro de número inteiro no Google Chrome antes de 13.0.782.215 em plataformas de 32 bits permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo matrizes uniformes.
CVE-2011-2828	O Google V8, usado no Google Chrome antes de 13.0.782.215, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que acionam uma gravação fora dos limites.
CVE-2011-2827	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 13.0.782.215 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à pesquisa de texto.
CVE-2011-2826	O Google Chrome anterior a 13.0.782.215 permite que invasores remotos contornem a Política de mesma origem por meio de vetores relacionados a origens vazias.
CVE-2011-2825	A vulnerabilidade de uso após a liberação no Google Chrome antes de 13.0.782.215 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo fontes personalizadas.
CVE-2011-2824	A vulnerabilidade de uso após a liberação no Google Chrome antes de 13.0.782.215 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo nós de contador.

Nome	Descrição
CVE-2011-2823	A vulnerabilidade de uso após a liberação no Google Chrome antes de 13.0.782.215 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo uma caixa de linha.
CVE-2011-2822	O Google Chrome anterior a 13.0.782.215 no Windows não analisa corretamente as URLs localizadas na linha de comando, que possui vetores de impacto e ataque não especificados.
CVE-2011-2821	A dupla vulnerabilidade livre na libxml2, conforme usada no Google Chrome antes de 13.0.782.215, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de uma expressão XPath criada.
CVE-2011-2819	O Google Chrome anterior a 13.0.782.107 permite que atacantes remotos contornem a Política de mesma origem por meio de vetores relacionados ao tratamento do URI de base.
CVE-2011-2818	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à renderização da caixa de exibição.
CVE-2011-2806	O Google Chrome anterior a 13.0.782.215 no Windows não lida adequadamente com dados de vértices, o que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados.
CVE-2011-2805	O Google Chrome anterior a 13.0.782.107 permite que atacantes remotos contornem a Política de mesma origem e conduzam ataques de injeção de script por meio de vetores não especificados.
CVE-2011-2804	O Google Chrome anterior a 13.0.782.107 não lida adequadamente com funções aninhadas em documentos PDF, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2011-2803	O Google Chrome anterior a 13.0.782.107 não lida corretamente com caminhos do Skia, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2802	O Google V8, usado no Google Chrome antes de 13.0.782.107, não realiza adequadamente pesquisas de const, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de um site criado.
CVE-2011-2801	A vulnerabilidade de uso após a liberação no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao carregador de quadros.

Nome	Descrição
CVE-2011-2800	O Google Chrome anterior a 13.0.782.107 permite que atacantes remotos obtenham informações potencialmente confidenciais sobre destinos de redirecionamento do lado do cliente por meio de um site criado.
CVE-2011-2799	A vulnerabilidade de uso após a liberação no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento do intervalo de HTML.
CVE-2011-2798	O Google Chrome anterior a 13.0.782.107 não restringe adequadamente o acesso a esquemas internos, o que permite que invasores remotos tenham um impacto não especificado por meio de um site criado.
CVE-2011-2797	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao armazenamento em cache de recursos.
CVE-2011-2796	A vulnerabilidade "use-after-free" no Skia, como usada no Google Chrome antes de 13.0.782.107, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2795	O Google Chrome anterior a 13.0.782.107 não impede as chamadas para funções em outros quadros, o que permite que atacantes remotos contornem as restrições de acesso pretendidas por meio de um site criado, relacionado a um "vazamento de função de quadro cruzado".
CVE-2011-2794	O Google Chrome anterior a 13.0.782.107 não executa corretamente a iteração de texto, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2793	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a seletores de mídia.
CVE-2011-2792	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à remoção de ponto flutuante.
CVE-2011-2791	A funcionalidade Componentes Internacionais para Unicode (ICU) no Google Chrome anterior a 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que açãoam uma gravação fora dos limites.
CVE-2011-2790	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 13.0.782.107 permite que invasores remotos causem uma

Nome	Descrição
	negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem estilos flutuantes.
CVE-2011-2789	A vulnerabilidade de uso após a liberação no Google Chrome antes de 13.0.782.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à instanciação do plug-in do Pepper.
CVE-2011-2788	O estouro de buffer na funcionalidade de serialização do inspetor no Google Chrome antes de 13.0.782.107 permite que invasores remotos assistidos pelo usuário tenham um impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2787	O Google Chrome anterior a 13.0.782.107 não aborda adequadamente os problemas de reencenação associados ao bloqueio de GPU, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2011-2786	O Google Chrome anterior a 13.0.782.107 não garante que a bolha de entrada de fala seja mostrada na tela do produto, o que pode facilitar para os invasores remotos fazer gravações de áudio por meio de uma página da Web criada que contenha um elemento INPUT.
CVE-2011-2785	A implementação das extensões no Google Chrome antes de 13.0.782.107 não valida corretamente o URL da página inicial, o que permite que invasores remotos tenham um impacto não especificado por meio de uma extensão criada.
CVE-2011-2784	O Google Chrome anterior a 13.0.782.107 permite que invasores remotos obtenham informações confidenciais por meio de uma solicitação para o log do programa GL, que revela um caminho local em uma entrada de log não especificada.
CVE-2011-2783	O Google Chrome anterior a 13.0.782.107 não garante que as instalações da extensão NPAPI no modo de desenvolvedor sejam confirmadas por uma caixa de diálogo do navegador, o que facilita para invasores remotos modificar a funcionalidade do produto por meio de uma extensão de cavalo de tróia.
CVE-2011-2782	A implementação de arrastar e soltar no Google Chrome antes de 13.0.782.107 no Linux não impõe adequadamente permissões para arquivos, o que permite que atacantes remotos assistidos por usuário ignorem as restrições de acesso pretendidas por meio de vetores não especificados.
CVE-2011-2761	O Google Chrome 14.0.794.0 não lida adequadamente com o recarregamento de uma página gerada em resposta a um POST, que permite que atacantes remotos assistidos por usuário causem uma negação de serviço (falha do aplicativo) por meio de um site criado relacionado aos métodos GetWidget.
CVE-2011-2604	O driver Intel G41 6.14.10.5355 no Windows XP SP3 permite que atacantes remotos causem uma negação de serviço (falha do sistema) por meio de uma página da Web criada acessada com o

Nome	Descrição
	Google Chrome ou o Mozilla Firefox, conforme demonstrado pelo exemplo da lots-of-polys .html página de teste no Khronos WebGL SDK.
CVE-2011-2603	O driver NVIDIA 9400M 6.2.6 no Mac OS X 10.6.7 permite que atacantes remotos causem uma negação de serviço (interceptação da área de trabalho) por meio de uma página da Web criada que é visitada com o Google Chrome ou Mozilla Firefox, conforme demonstrado pelo site polys-example.html página de teste no Khronos WebGL SDK.
CVE-2011-2602	O driver NVIDIA Geforce 310 6.14.12.7061 no Windows XP SP3 permite que atacantes remotos causem uma negação de serviço (falha do sistema) por meio de uma página da Web criada que é visitada com o Google Chrome ou o Mozilla Firefox, conforme demonstrado pelos lotes de polys. exemplo.html página de teste no Khronos WebGL SDK.
CVE-2011-2601	A funcionalidade de suporte a GPU no Mac OS X não restringe adequadamente o tempo de renderização, o que permite que atacantes remotos causem uma negação de serviço (interrupção de desktop) por meio de vetores envolvendo WebGL e (1) programas de sombreamento ou (2) geometria 3D complexa, conforme demonstrado por usando o Mozilla Firefox ou o Google Chrome para visitar a página de teste lots-of-polys-example.html no Khronos WebGL SDK.
CVE-2011-2600	A funcionalidade de suporte da GPU no Windows XP não restringe adequadamente o tempo de renderização, o que permite que atacantes remotos causem uma negação de serviço (falha do sistema) por meio de vetores envolvendo WebGL e (1) programas de sombreamento ou (2) geometria 3D complexa, conforme demonstrado pelo uso Mozilla Firefox ou Google Chrome para visitar a página de teste lots-of-polys-example.html no Khronos WebGL SDK.
CVE-2011-2599	O Google Chrome 11 não bloqueia o uso de uma imagem de domínio cruzado como uma textura WebGL, que permite que atacantes remotos obtenham cópias aproximadas de imagens arbitrárias por meio de um ataque de sincronização envolvendo um fragmento de fragmento WebGL criado.
CVE-2011-2361	A implementação da caixa de diálogo Autenticação básica no Google Chrome antes de 13.0.782.107 não lida adequadamente com strings, o que pode facilitar a captura de credenciais por um site criado por invasores remotos.
CVE-2011-2360	O Google Chrome anterior a 13.0.782.107 não garante que o usuário seja solicitado antes do download de um arquivo perigoso, o que facilita aos invasores remotos evitar as restrições de conteúdo pretendidas por meio de um site criado.
CVE-2011-2359	O Google Chrome anterior a 13.0.782.107 não acompanha corretamente caixas de linha durante a renderização, o que permite que atacantes remotos causem uma negação de serviço ou

Nome	Descrição
	possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-2358	O Google Chrome anterior a 13.0.782.107 não garante que as instalações de extensão sejam confirmadas por uma caixa de diálogo do navegador, o que facilita para os invasores remotos modificar a funcionalidade do produto por meio de uma extensão de cavalo de Tróia.
CVE-2011-2351	A vulnerabilidade de uso após a liberação no Google Chrome antes de 12.0.742.112 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem elementos de uso do SVG.
CVE-2011-2350	O analisador de HTML do Google Chrome anterior a 12.0.742.112 não aborda de forma adequada os "problemas de vida útil e reentrância", o que permite que atacantes remotos causem uma negação de serviço ou possam ter outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2349	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 12.0.742.112 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à seleção de texto.
CVE-2011-2348	O Google V8, usado no Google Chrome antes de 12.0.742.112, realiza uma verificação de limites incorreta, que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2347	O Google Chrome anterior a 12.0.742.112 não processa adequadamente sequências de tokens de CSS (Cascading Style Sheets), o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-2346	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes de 12.0.742.112 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo fontes SVG.
CVE-2011-2345	A implementação de NPAPI no Google Chrome anterior a 12.0.742.112 não lida corretamente com strings, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-2342	A implementação do DOM no Google Chrome antes de 12.0.742.91 permite que invasores remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2011-2332	O Google V8, usado no Google Chrome antes de 12.0.742.91, permite que invasores remotos ignorem a Política de mesma origem por meio de vetores não especificados.

Nome	Descrição
CVE-2011-2171	Vulnerabilidade não especificada no pacote dbugs no Google Chrome OS anterior à R12 0.12.433.38 Beta tem impacto e vetores de ataque desconhecidos.
CVE-2011-2170	O Google Chrome OS anterior à R12 0.12.433.38 Beta, quando o modo Convidado está ativado, não impede alterações na página sobre: sinalizadores, que possui vetores de impacto locais e de impacto não especificados.
CVE-2011-2169	O Google Chrome OS antes do R12 0.12.433.38 Beta permite que usuários locais obtenham privilégios criando um arquivo /var/lib/chromeos-aliases.conf e colocando comandos nele.
CVE-2011-2162	Várias vulnerabilidades não especificadas no FFmpeg 0.4.x até 0.6.x, como usadas no MPlayer 1.0 e em outros produtos, no Mandriva Linux 2009.0, 2010.0 e 2010.1; Servidor Corporativo 4.0 (também conhecido como CS4.0); e o Mandriva Enterprise Server 5 (também conhecido como MES5) tem vetores de impacto e ataque desconhecidos, relacionados a problemas "originalmente descobertos por desenvolvedores do Google Chrome".
CVE-2011-2075	A vulnerabilidade não especificada no Google Chrome 11.0.696.65 no Windows 7 SP1 permite que atacantes remotos executem código arbitrário por meio de vetores desconhecidos. OBSERVAÇÃO: a partir de 20110510, a única divulgação é um aviso vago, possivelmente relacionado a várias vulnerabilidades ou vários produtos. No entanto, como é de um pesquisador conhecido, está sendo atribuído um identificador CVE para fins de rastreamento.
CVE-2011-1819	O Google Chrome anterior a 12.0.742.91 permite que atacantes remotos executem injeção não especificada em uma página chrome:// por meio de vetores relacionados a extensões.
CVE-2011-1818	A vulnerabilidade "usar-depois-livre" no carregador de imagens do Google Chrome antes de 12.0.742.91 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1817	O Google Chrome anterior a 12.0.742.91 não implementa adequadamente a exclusão do histórico, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1816	A vulnerabilidade "usar-depois-de-livre" nas ferramentas do desenvolvedor no Google Chrome antes de 12.0.742.91 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1815	O Google Chrome anterior a 12.0.742.91 permite que invasores remotos injetem scripts em uma guia por meio de vetores relacionados a extensões.
CVE-2011-1814	O Google Chrome anterior a 12.0.742.91 tenta ler dados de um ponteiro não inicializado, o que permite que atacantes remotos

Nome	Descrição
	causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1813	O Google Chrome anterior a 12.0.742.91 não implementa adequadamente a estrutura para extensões, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1812	O Google Chrome anterior a 12.0.742.91 permite que atacantes remotos contornem as restrições de acesso pretendidas por meio de vetores relacionados a extensões.
CVE-2011-1811	O Google Chrome anterior a 12.0.742.91 não lida adequadamente com um grande número de envios de formulários, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2011-1810	A implementação das CSS (Cascading Style Sheets) no Google Chrome antes de 12.0.742.91 não restringe adequadamente o acesso ao histórico de visitas, o que permite que atacantes remotos obtenham informações confidenciais por meio de vetores não especificados.
CVE-2011-1809	A vulnerabilidade de uso após a liberação no recurso de acessibilidade do Google Chrome antes de 12.0.742.91 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1808	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 12.0.742.91 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a cálculos incorretos de números inteiros durante o manuseio de flutuante.
CVE-2011-1807	O Google Chrome anterior a 11.0.696.71 não lida corretamente com blobs, o que permite que atacantes remotos executem código arbitrário por meio de vetores não especificados que acionam uma gravação fora dos limites.
CVE-2011-1806	O Google Chrome anterior a 11.0.696.71 não implementa adequadamente o buffer de comando da GPU, que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória) por meio de vetores não especificados.
CVE-2011-1804	rendering / RenderBox.cpp no WebCore no WebKit antes de r86862, como usado no Google Chrome antes de 11.0.696.71, não renderiza corretamente os floats, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1801	A vulnerabilidade não especificada no Google Chrome anterior a 11.0.696.71 permite que invasores remotos ignorem o bloqueador de pop-up por meio de vetores desconhecidos.

Nome	Descrição
CVE-2011-1800	Vários transbordamentos de números inteiros na implementação de Filtros SVG no WebCore no WebKit no Google Chrome antes de 11.0.696.68 permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1799	O Google Chrome anterior a 11.0.696.68 não executa corretamente conjuntos de variáveis durante a interação com o mecanismo do WebKit, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1798	rendering / svg / RenderSVGText.cpp no WebCore no WebKit no Google Chrome antes de 11.0.696.65 não executa adequadamente uma conversão de uma variável não especificada durante uma tentativa de manipular um bloco filho, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente ter outro impacto desconhecido por meio de um elemento de texto criado em um documento SVG.
CVE-2011-1797	O WebKit, usado no Apple Safari antes do 5.0.6, permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória e falha de aplicativo) através de um site criado, uma vulnerabilidade diferente das outras CVEs listadas no APPLE-SA -2011-07-20-1.
CVE-2011-1796	A vulnerabilidade use-after-free na função FrameView :: calculateScrollbarModesForLayout na página / FrameView.cpp no WebCore no WebKit no Google Chrome antes de 11.0.696.65 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado via Código JavaScript criado que chama o método removeChild durante a interação com um elemento FRAME.
CVE-2011-1795	Inferior inteiro na função HTMLFormElement :: removeFormElement em html / HTMLFormElement.cpp no WebCore no WebKit no Google Chrome antes de 11.0.696.65 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de um documento HTML criado contendo um elemento FORM.
CVE-2011-1794	O estouro de inteiro na função FilterEffect :: copyImageBytes em platform / graphics / filters / FilterEffect.cpp na implementação do filtro SVG no WebCore no WebKit no Google Chrome antes de 11.0.696.65 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente não especificou outro impacto através de dimensões criadas.
CVE-2011-1793	rendering / svg / RenderSVGResourceFilter.cpp no WebCore no WebKit no Google Chrome antes de 11.0.696.65 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente não tenham outro impacto por meio de um documento SVG criado que leve a um "ponteiro antigo".

Nome	Descrição
CVE-2011-1691	A função counterToCSSValue em CSSComputedStyleDeclaration.cpp na implementação das CSS (Cascading Style Sheets) no WebCore no WebKit antes do r82222, como usado no Google Chrome antes de 11.0.696.43 e outros produtos, não manipula adequadamente o acesso ao (1) counterIncrement e (2) Atributos do counterReset de dados CSSStyleDeclaration fornecidos por uma chamada de método getComputedStyle, que permite que atacantes remotos causem uma negação de serviço (desreferenciamento de ponteiro NULL e falha de aplicativo) por meio de código JavaScript criado.
CVE-2011-1465	A implementação do SPDY em net / http / http_network_transaction.cc no Google Chrome anterior a 11.0.696.14 drena os corpos das respostas SPDY, o que pode permitir que servidores SPDY remotos causem uma negação de serviço (saída de aplicativo) cancelando um fluxo.
CVE-2011-1456	O Google Chrome anterior a 11.0.696.57 não lida corretamente com formulários PDF, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "indicadores obsoletos".
CVE-2011-1455	O Google Chrome anterior a 11.0.696.57 não processa adequadamente documentos PDF com codificação multiparte, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de um documento criado.
CVE-2011-1454	A vulnerabilidade "use-after-free" na funcionalidade de manipulação de ID do DOM no Google Chrome anterior a 11.0.696.57 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento HTML criado.
CVE-2011-1452	O Google Chrome anterior a 11.0.696.57 permite que invasores remotos assistidos por usuários falsifiquem a barra de URL por meio de vetores que envolvam um redirecionamento e uma recarga manual.
CVE-2011-1451	O Google Chrome anterior a 11.0.696.57 não manipula adequadamente mapas DOM id, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "ponteiros pendentes".
CVE-2011-1450	O Google Chrome anterior a 11.0.696.57 não apresenta adequadamente diálogos de arquivos, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "indicadores pendentes".
CVE-2011-1449	A vulnerabilidade "usar-depois-livre" na implementação do WebSockets no Google Chrome antes de 11.0.696.57 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de

Nome	Descrição
	vetores desconhecidos.
CVE-2011-1448	O Google Chrome anterior a 11.0.696.57 não realiza cálculos de altura corretamente, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1447	O Google Chrome anterior a 11.0.696.57 não lida corretamente com listas suspensas, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro ultrapassado".
CVE-2011-1446	O Google Chrome anterior a 11.0.696.57 permite que atacantes remotos falsifiquem a barra de URL por meio de vetores envolvendo (1) um erro de navegação ou (2) uma carga interrompida.
CVE-2011-1445	O Google Chrome anterior a 11.0.696.57 não manipula corretamente documentos SVG, o que permite que invasores remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-1444	A condição de corrida na implementação do lançador de sandbox no Google Chrome antes de 11.0.696.57 no Linux permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1443	O Google Chrome anterior a 11.0.696.57 não implementa adequadamente as camadas, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "indicadores obsoletos".
CVE-2011-1442	O Google Chrome anterior a 11.0.696.57 não lida adequadamente com eventos de mutação, o que permite que invasores remotos causem uma negação de serviço (corrupção na árvore de nós) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1441	O Google Chrome anterior a 11.0.696.57 não executa adequadamente uma conversão de uma variável não especificada durante o manuseio de listas de seleção flutuantes, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento HTML criado.
CVE-2011-1440	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 11.0.696.57 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao elemento ruby e sequências de token CSS (Cascading Style Sheets).
CVE-2011-1439	O Google Chrome anterior ao 11.0.696.57 no Linux não isola adequadamente os processos do renderizador, que possui vetores

Nome	Descrição
	de impacto e ataque remotos não especificados.
CVE-2011-1438	O Google Chrome anterior a 11.0.696.57 permite que invasores remotos contornem a Política de mesma origem por meio de vetores que envolvem blobs.
CVE-2011-1437	Vários transbordos de números inteiros no Google Chrome anteriores a 11.0.696.57 permitem que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à renderização flutuante.
CVE-2011-1436	O Google Chrome anterior ao 11.0.696.57 no Linux não interage adequadamente com o X Window System, que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2011-1435	O Google Chrome anterior a 11.0.696.57 não implementa adequadamente a permissão de guias para extensões, o que permite que atacantes remotos leiam arquivos locais por meio de uma extensão criada.
CVE-2011-1434	O Google Chrome anterior a 11.0.696.57 não garante segurança de thread durante o tratamento de dados MIME, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1413	O Google Chrome anterior ao 10.0.648.127 no Linux não atenua adequadamente uma falha não especificada em um servidor X, que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores que envolvam mensagens longas.
CVE-2011-1398	A função sapi_header_op em main / SAPI.c em PHP antes de 5.3.11 e 5.4.x antes de 5.4.0RC2 não verifica sequências% 0D (também caracteres de retorno de carro), o que permite que atacantes remotos contornem um mecanismo de proteção de divisão de resposta HTTP por meio de uma URL criada, relacionada à interação imprópria entre a função de cabeçalho do PHP e determinados navegadores, conforme demonstrado pelo Internet Explorer e pelo Google Chrome.
CVE-2011-1306	A vulnerabilidade não especificada no aplicativo Scratchpad no Google Chrome OS anterior à R10 0.10.156.46 Beta tem impacto e vetores de ataque desconhecidos.
CVE-2011-1305	A condição de corrida no Google Chrome anterior a 11.0.696.57 no Linux e Mac OS X permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a listas vinculadas e a um banco de dados.
CVE-2011-1304	A vulnerabilidade não especificada no Google Chrome anterior a 11.0.696.57 permite que atacantes remotos ignorem o bloqueador de pop-ups por meio de vetores relacionados a plug-ins.

Nome	Descrição
CVE-2011-1303	O Google Chrome anterior a 11.0.696.57 não lida corretamente com objetos flutuantes, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1302	O estouro de buffer baseado em heap no processo da GPU no Google Chrome antes de 10.0.648.205 permite que atacantes remotos executem código arbitrário por meio de vetores desconhecidos.
CVE-2011-1301	A vulnerabilidade de uso após a liberação no processo da GPU no Google Chrome antes de 10.0.648.205 permite que atacantes remotos executem código arbitrário por meio de vetores desconhecidos.
CVE-2011-1300	A função Program :: getActiveUniformMaxLength em libGLESv2 / Program.cpp em libGLESv2.dll na biblioteca WebGLES no mecanismo de camada de gráficos quase nativos (ANGLE), como usado no Mozilla Firefox 4.x antes de 4.0.1 no Windows e no processo de GPU em O Google Chrome, antes de 10.0.648.205 no Windows, permite que atacantes remotos executem código arbitrário por meio de vetores não especificados, relacionados a um erro "off-by-three".
CVE-2011-1296	O Google Chrome anterior a 10.0.648.204 não processa corretamente o texto SVG, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1295	O WebKit, como usado no Google Chrome antes de 10.0.648.204 e o Apple Safari anterior à 5.0.6, não manipula adequadamente o parentesco de nós, que permite que invasores remotos causem uma negação de serviço (corrupção de árvore DOM) e realizem scripts entre sites (XSS) ataques, ou possivelmente não ter especificado outro impacto através de vetores desconhecidos.
CVE-2011-1294	O Google Chrome anterior a 10.0.648.204 não processa adequadamente sequências de tokens de CSS (Cascading Style Sheets), o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1293	A vulnerabilidade "usar-depois-livre" na implementação do HTMLCollection no Google Chrome antes de 10.0.648.204 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1292	A vulnerabilidade "usar-depois-livre" na implementação do carregador de quadros no Google Chrome antes de 10.0.648.204 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de

Nome	Descrição
CVE-2011-1291	vetores desconhecidos.
CVE-2011-1290	O Google Chrome anterior a 10.0.648.204 não lida corretamente com strings de base, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos, relacionados a um "erro de buffer".
CVE-2011-1290	O estouro de número inteiro no WebKit, usado no BlackBerry Torch 9800 da Research In Motion (RIM) com firmware 6.0.0.246, no Google Chrome antes de 10.0.648.133, e no Apple Safari anterior à 5.0.5, permite que atacantes remotos executem código arbitrário por meio de desconhecido vetores relacionados a CSS "style handling", nodesets e um valor de comprimento, conforme demonstrado por Vincenzo Iozzo, Willem Pinckaers e Ralf-Philipp Weinmann durante uma competição Pwn2Own no CanSecWest 2011.
CVE-2011-1286	O Google V8, conforme usado no Google Chrome antes de 10.0.648.127, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que acionam o acesso incorreto à memória.
CVE-2011-1285	A funcionalidade de expressão regular no Google Chrome anterior a 10.0.648.127 não implementa corretamente a reentrada, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1204	O Google Chrome anterior a 10.0.648.127 não lida corretamente com atributos, o que permite que atacantes remotos causem uma negação de serviço (corrupção de árvore DOM) ou possivelmente tenham outro impacto não especificado por meio de um documento criado.
CVE-2011-1203	O Google Chrome anterior a 10.0.648.127 não manipula corretamente os cursores SVG, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1202	A função xsItGenerateIdFunction em functions.c na libxslt 1.1.26 e anterior, como usada no Google Chrome antes de 10.0.648.127 e outros produtos, permite que atacantes remotos obtenham informações potencialmente confidenciais sobre endereços de memória de heap por meio de um documento XML contendo uma chamada para o XSLT função XPath generate-id.
CVE-2011-1201	A implementação de contexto no WebKit, como usada no Google Chrome antes de 10.0.648.127, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1200	O Google Chrome anterior a 10.0.648.127 não executa

Nome	Descrição
	adequadamente uma conversão de uma variável não especificada durante a renderização de texto, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto desconhecido por meio de um documento criado.
CVE-2011-1199	O Google Chrome anterior a 10.0.648.127 não lida corretamente com objetos DataView, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou, possivelmente, tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1198	A funcionalidade de vídeo no Google Chrome anterior a 10.0.648.127 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que acionam o uso de uma "estrutura fora dos limites" malformada.
CVE-2011-1197	O Google Chrome anterior a 10.0.648.127 não executa corretamente a pintura de tabela, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1196	A implementação do contêiner OGG no Google Chrome anterior a 10.0.648.127 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que acionam uma gravação fora dos limites.
CVE-2011-1195	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 10.0.648.127 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao "tratamento da vida útil do script do documento".
CVE-2011-1194	Diversas vulnerabilidades não especificadas no Google Chrome anteriores a 10.0.648.127 permitem que atacantes remotos ignorem o bloqueador de pop-ups por meio de vetores desconhecidos.
CVE-2011-1193	O Google V8, usado no Google Chrome antes de 10.0.648.127, permite que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2011-1192	O Google Chrome anterior ao 10.0.648.127 no Linux não lida corretamente com intervalos Unicode, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-1191	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 10.0.648.127 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento de URLs DOM.
CVE-2011-1190	A implementação do Web Workers no Google Chrome anterior a 10.0.648.127 permite que invasores remotos contornem a Política

Nome	Descrição
	de mesma origem por meio de vetores não especificados, relacionados a um "vazamento de mensagem de erro".
CVE-2011-1189	O Google Chrome anterior a 10.0.648.127 não executa corretamente o layout da caixa, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "nó obsoleto".
CVE-2011-1188	O Google Chrome anterior a 10.0.648.127 não manipula corretamente os nós de contador, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1187	O Google Chrome anterior a 10.0.648.127 permite que invasores remotos contornem a Política de mesma origem por meio de vetores não especificados, relacionados a "vazamento de mensagens de erro".
CVE-2011-1186	O Google Chrome anterior ao 10.0.648.127 no Linux não lida adequadamente com a execução paralela de chamadas ao método de impressão, o que pode permitir que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de código JavaScript criado.
CVE-2011-1185	O Google Chrome anterior a 10.0.648.127 não impede (1) a navegação e (2) fecha as operações na localização superior de um quadro de área restrita, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-1125	O Google Chrome anterior a 9.0.597.107 não executa corretamente o layout, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1124	A vulnerabilidade "usar-depois-de-graça" no Google Chrome antes da versão 9.0.597.107 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a plug-ins bloqueados.
CVE-2011-1123	O Google Chrome anterior a 9.0.597.107 não restringe adequadamente o acesso a funções de extensão interna, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-1122	A implementação do WebGL no Google Chrome antes de 9.0.597.107 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados, também conhecidos como Edição 71960.
CVE-2011-1121	O estouro de número inteiro no Google Chrome antes da versão 9.0.597.107 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo um elemento TEXTAREA.

Nome	Descrição
CVE-2011-1120	A implementação do WebGL no Google Chrome antes de 9.0.597.107 permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados, também conhecidos como Edição 71717.
CVE-2011-1119	O Google Chrome anterior à 9.0.597.107 não determina adequadamente a orientação do dispositivo, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1118	O Google Chrome anterior à 9.0.597.107 não manipula corretamente os elementos TEXTAREA, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de um documento HTML criado.
CVE-2011-1117	O Google Chrome anterior à 9.0.597.107 não manipula corretamente documentos XHTML, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "nós obsoletos".
CVE-2011-1116	O Google Chrome anterior à 9.0.597.107 não lida corretamente com animações SVG, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1115	O Google Chrome anterior a 9.0.597.107 não processa tabelas corretamente, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1114	O Google Chrome anterior à 9.0.597.107 não lida corretamente com tabelas, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "nó obsoleto".
CVE-2011-1113	O Google Chrome anterior a 9.0.597.107 em plataformas Linux de 64 bits não executa corretamente a desserialização de pickles, o que permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-1112	O Google Chrome anterior à 9.0.597.107 não executa corretamente a renderização SVG, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1111	O Google Chrome anterior à 9.0.597.107 não implementa adequadamente os controles de formulários, o que permite que invasores remotos causem uma negação de serviço (falha do

Nome	Descrição
	aplicativo) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-1110	O Google Chrome anterior à 9.0.597.107 não implementa adequadamente regras de quadros principais, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1109	O Google Chrome anterior a 9.0.597.107 não processa os nós adequadamente nas folhas de estilo CSS (Cascading Style Sheets), o que permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-1108	O Google Chrome anterior à 9.0.597.107 não implementa corretamente as caixas de diálogo JavaScript, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou, possivelmente, não tenham outro impacto não especificado por meio de um documento HTML criado.
CVE-2011-1107	A vulnerabilidade não especificada no Google Chrome anterior à 9.0.597.107 permite que invasores remotos falsifiquem a barra de URL por meio de vetores desconhecidos.
CVE-2011-1071	A Biblioteca GNU C (também conhecida como glibc ou libc6) antes de 2.12.2 e GLIBC Incorporado (EGLIBC) permite que atacantes dependentes de contexto executem código arbitrário ou causem uma negação de serviço (consumo de memória) através de uma longa string UTF8 que é usada em um fnmatch chamada, também chamada de "ataque de extensão de pilha", um problema relacionado ao CVE-2010-2898, CVE-2010-1917 e CVE-2007-4782, conforme relatado originalmente para uso desta biblioteca pelo Google Chrome.
CVE-2011-1059	A vulnerabilidade de usar o after-free no WebCore no WebKit antes do r77705, como usado no Google Chrome antes de 11.0.672.2 e outros produtos, permite que atacantes remotos assistidos causem uma negação de serviço (falha no aplicativo) ou possivelmente não tenham outro impacto causado por vetores que incitam um usuário a reenviar um formulário, relacionado ao manuseio inadequado de itens provisórios pelo componente HistoryController, também conhecido como rdar problem 8938557.
CVE-2011-1042	A vulnerabilidade use-after-free em flimflamd em flimflam no Google Chrome OS antes de 0.9.130.14 Beta permite que atacantes remotos assistidos por usuário causem uma negação de serviço (falha no daemon) fornecendo o nome de uma rede WiFi oculta que não responde à conexão tentativas.
CVE-2011-0985	O Google Chrome anterior a 9.0.597.94 não realiza corretamente a finalização do processo após o esgotamento da memória, que possui vetores de impacto e ataque remoto não especificados.
CVE-2011-0984	O Google Chrome anterior a 9.0.597.94 não lida corretamente com plug-ins, o que permite que atacantes remotos causem uma

Nome	Descrição
	negação de serviço (leitura fora dos limites) por meio de vetores não especificados.
CVE-2011-0983	O Google Chrome anterior a 9.0.597.94 não manipula corretamente blocos anônimos, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-0982	A vulnerabilidade "usar-depois-livre" no Google Chrome antes da versão 9.0.597.94 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores envolvendo faces de fontes SVG.
CVE-2011-0981	O Google Chrome anterior à versão 9.0.597.94 não realiza adequadamente a manipulação de eventos para animações, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-0784	A condição de corrida no Google Chrome anterior à 9.0.597.84 permite que atacantes remotos executem código arbitrário por meio de vetores relacionados ao áudio.
CVE-2011-0783	A vulnerabilidade não especificada no Google Chrome anterior à 9.0.597.84 permite que invasores remotos assistidos por usuário causem uma negação de serviço (falha do aplicativo) por meio de vetores que envolvam uma "configuração de volume inválido".
CVE-2011-0782	O Google Chrome anterior a 9.0.597.84 no Mac OS X não atenua adequadamente uma falha não especificada nas bibliotecas SSL do Mac OS X 10.5, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores desconhecidos.
CVE-2011-0781	O Google Chrome anterior à 9.0.597.84 não processa adequadamente a fusão do perfil de preenchimento automático, que possui vetores de impacto e ataque remotos não especificados.
CVE-2011-0780	O manipulador de eventos do PDF no Google Chrome anterior à 9.0.597.84 não interage adequadamente com operações de impressão, o que permite que atacantes remotos assistidos por usuário causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-0779	O Google Chrome anterior à 9.0.597.84 não manipula adequadamente uma chave ausente em uma extensão, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de uma extensão criada.
CVE-2011-0778	O Google Chrome anterior a 9.0.597.84 não restringe adequadamente as operações de arrastar e soltar, o que pode permitir que atacantes remotos contornem a Política de mesma origem por meio de vetores não especificados.
CVE-2011-0777	A vulnerabilidade "usar-depois-de-graça" no Google Chrome

Nome	Descrição
	anterior à 9.0.597.84 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao carregamento de imagens.
CVE-2011-0776	A implementação do sandbox no Google Chrome antes de 9.0.597.84 no Mac OS X pode permitir que atacantes remotos obtenham informações potencialmente confidenciais sobre arquivos locais por meio de vetores relacionados à chamada do sistema stat.
CVE-2011-0485	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não lidam adequadamente com dados de fala, o que permite que atacantes remotos executem código arbitrário por meio de vetores não especificados que levam a um "ponteiro obsoleto".
CVE-2011-0484	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não realizam corretamente a remoção do nó DOM, o que permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "nó de renderização obsoleto".
CVE-2011-0483	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não executam adequadamente um elenco de uma variável não especificada durante o processamento de vídeo, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2011-0482	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não executam adequadamente um elenco de uma variável não especificada durante o manuseio de âncoras, o que permite que invasores remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de um documento HTML criado.
CVE-2011-0481	O estouro de buffer no Google Chrome anterior a 8.0.552.237 e o Chrome OS anterior a 8.0.552.344 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao sombreamento de PDF.
CVE-2011-0480	Vários buffer overflows em vorbis_dec.c no decodificador Vorbis no FFmpeg, como usado no Google Chrome antes de 8.0.552.237 e no Chrome OS antes de 8.0.552.344, permitem que atacantes remotos causem uma negação de serviço (corrupção de memória e falha de aplicativo) ou possivelmente Outro impacto não especificado por meio de um arquivo WebM criado, relacionado a buffers para (1) o piso do canal e (2) o resíduo do canal.
CVE-2011-0479	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não interagem adequadamente com as extensões, o que permite que invasores remotos causem uma negação de serviço por meio de uma extensão criada que aciona um ponteiro

Nome	Descrição
não inicializado.	
CVE-2011-0478	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não manipulam adequadamente os elementos de uso SVG, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro antigo".
CVE-2011-0477	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não manipulam adequadamente uma incompatibilidade nos tamanhos de quadros de vídeo, o que permite que atacantes remotos causem uma negação de serviço (acesso incorreto à memória) ou possivelmente não tenham outro impacto por meio de vetores desconhecidos.
CVE-2011-0476	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 permitem que invasores remotos causem uma negação de serviço (corrupção de memória da pilha) ou possivelmente tenham outro impacto não especificado por meio de um documento PDF que aciona um erro de falta de memória.
CVE-2011-0475	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 8.0.552.237 e o Chrome OS anterior a 8.0.552.344 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de um documento PDF.
CVE-2011-0474	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não manipulam adequadamente sequências de tokens de CSS (Cascading Style Sheets) em conjunto com cursores, o que permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores desconhecidos. levar a um "ponteiro obsoleto".
CVE-2011-0473	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não manipulam adequadamente sequências de tokens de CSS (Cascading Style Sheets) em conjunto com elementos CANVAS, o que permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de vetores desconhecidos que levam a um "ponteiro obsoleto".
CVE-2011-0472	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anteriores a 8.0.552.344 não manipulam adequadamente a impressão de documentos PDF, o que permite que invasores remotos assistidos por usuário causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado documento da página.
CVE-2011-0471	A implementação da iteração de nó no Google Chrome antes do 8.0.552.237 e do Chrome OS antes de 8.0.552.344 não manipula corretamente os ponteiros, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.

Nome	Descrição
CVE-2011-0470	O Google Chrome anterior a 8.0.552.237 e o Chrome OS anterior a 8.0.552.344 não lidam adequadamente com a notificação de extensões, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2010-5073	A implementação do JavaScript no Google Chrome 4 não restringe adequadamente o conjunto de valores contidos no objeto retornado pelo método getComputedStyle, que permite que atacantes remotos obtenham informações confidenciais sobre páginas da Web visitadas chamando esse método. NOTA: isso pode se sobrepor ao CVE-2010-5070.
CVE-2010-5069	A implementação de CSS (Cascading Style Sheets) no Google Chrome 4 não lida corretamente com a pseudo-classe: visitada, que permite que atacantes remotos obtenham informações confidenciais sobre páginas da Web visitadas por meio de um documento HTML criado. NOTA: isso pode se sobrepor ao CVE-2010-2264.
CVE-2010-4578	O Google Chrome anterior a 8.0.552.224 e o Chrome OS anteriores a 8.0.552.343 não executam adequadamente o tratamento de cursor, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos que levam a "indicadores obsoletos".
CVE-2010-4577	A função CSSParser :: parseFontFaceSrc em WebCore / css / CSSParser.cpp no WebKit, como usada no Google Chrome antes de 8.0.552.224, Chrome OS antes de 8.0.552.343, webkitgtk antes de 1.2.6, e outros produtos não analisa corretamente as Folhas de Estilo em Cascata Sequências de tokens (CSS), que permitem que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de uma fonte local trabalhada, relacionada a "Confusão de tipo".
CVE-2010-4576	browser / worker_host / message_port_dispatcher.cc no Google Chrome anterior a 8.0.552.224 e o Chrome OS anterior a 8.0.552.343 não manipula corretamente determinadas chamadas de postMessage, o que permite que atacantes remotos causem uma negação de serviço (desreferenciação de ponteiro NULL e falha de aplicativo) por meio de JavaScript criado código que cria um trabalhador da web.
CVE-2010-4575	A função ThemeInstalledInfoBarDelegate :: Observe em browser / extensions / theme_installed_infobar_delegate.cc no Google Chrome anterior a 8.0.552.224 e o Chrome OS anterior a 8.0.552.343 não manipula corretamente a interação incorreta da guia por uma extensão, o que permite que invasores remotos assistidos causem uma negação de serviço (falha de aplicativo) por meio de uma extensão criada.
CVE-2010-4574	A função Pickle :: Pickle em base / pickle.cc no Google Chrome anterior a 8.0.552.224 e o Chrome OS anterior a 8.0.552.343 em plataformas Linux de 64 bits não executa corretamente a

Nome	Descrição
	aritmética de ponteiro, o que permite que atacantes remotos ignorem a validação de desserialização de mensagens causar uma negação de serviço ou possivelmente não ter outro impacto, através de dados inválidos de pickle.
CVE-2010-4494	A dupla vulnerabilidade livre no libxml2 2.7.8 e outras versões, como usada no Google Chrome antes de 8.0.552.215 e outros produtos, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao tratamento do XPath.
CVE-2010-4493	A vulnerabilidade de uso após a liberação no Google Chrome antes do 8.0.552.215 permite que atacantes remotos causem uma negação de serviço por meio de vetores relacionados ao gerenciamento de eventos de arrastamento do mouse.
CVE-2010-4492	A vulnerabilidade de uso após a liberação no Google Chrome antes do 8.0.552.215 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem animações SVG.
CVE-2010-4491	O Google Chrome anterior a 8.0.552.215 não restringe adequadamente extensões com privilégios, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) por meio de uma extensão criada.
CVE-2010-4490	O Google Chrome anterior a 8.0.552.215 permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de conteúdo de vídeo malformado que aciona um erro de indexação.
CVE-2010-4489	O libvpx, como usado no Google Chrome antes do 8.0.552.215 e possivelmente outros produtos, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites) por meio de um vídeo WebM criado. NOTA: esta vulnerabilidade existe devido a uma regressão.
CVE-2010-4488	O Google Chrome anterior a 8.0.552.215 não lida corretamente com a autenticação de proxy HTTP, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2010-4487	A vulnerabilidade incompleta da lista negra no Google Chrome anterior a 8.0.552.215 no Linux e no Mac OS X permite que invasores remotos tenham um impacto não especificado por meio de um "arquivo perigoso".
CVE-2010-4486	A vulnerabilidade "usar-depois-livre" no Google Chrome antes do 8.0.552.215 permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados ao manuseio do histórico.
CVE-2010-4485	O Google Chrome anterior a 8.0.552.215 não restringe adequadamente a geração de diálogos de arquivos, o que permite que atacantes remotos causem uma negação de serviço (facilidade de uso reduzida e possível falha do aplicativo) por meio de um site

Nome	Descrição
	criado.
CVE-2010-4484	O Google Chrome anterior a 8.0.552.215 não lida adequadamente com bancos de dados HTML5, o que permite que invasores causem uma negação de serviço (falha de aplicativo) por meio de vetores não especificados.
CVE-2010-4483	O Google Chrome anterior a 8.0.552.215 não restringe adequadamente o acesso de leitura a vídeos derivados de elementos CANVAS, o que permite que atacantes remotos contornem a Política de mesma origem e obtenham dados de vídeo potencialmente confidenciais por meio de um site criado.
CVE-2010-4482	A vulnerabilidade não especificada no Google Chrome anterior a 8.0.552.215 permite que invasores remotos ignorem o bloqueador de pop-up por meio de vetores desconhecidos.
CVE-2010-4206	Erro de índice de matriz na função FEBlend :: apply em WebCore / platform / graphics / filters / FEBlend.cpp no WebKit, como usado no Google Chrome antes de 7.0.517.44, webkitgtk antes de 1.2.6 e outros produtos, permite que atacantes remotos causem uma negação de serviço e possivelmente executar código arbitrário por meio de um documento SVG criado, relacionado a efeitos na aplicação de filtros.
CVE-2010-4205	O Google Chrome anterior à versão 7.0.517.44 não manipula adequadamente os tipos de dados de objetos de evento, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-4204	O Webkit, usado no Google Chrome antes de 7.0.517.44, o webkitgtk antes de 1.2.6 e outros produtos acessam um objeto de quadro depois que esse objeto foi destruído, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores desconhecidos.
CVE-2010-4203	O WebM libvpx (também conhecido como VP8 Codec SDK) anterior a 0.9.5, como usado no Google Chrome antes de 7.0.517.44, permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente executar código arbitrário via quadros inválidos.
CVE-2010-4202	Vários overflows inteiros no Google Chrome anteriores a 7.0.517.44 no Linux permitem que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de uma fonte criada.
CVE-2010-4201	A vulnerabilidade de uso após a liberação no Google Chrome anterior a 7.0.517.44 permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores que envolvem seleções de controle de texto.
CVE-2010-4199	O Google Chrome anterior à versão 7.0.517.44 não executa adequadamente uma conversão de uma variável não especificada

Nome	Descrição
	durante o processamento de um elemento de uso SVG, o que permite que invasores remotos causem uma negação de serviço ou tenham outro impacto não especificado por meio de um documento SVG criado.
CVE-2010-4198	WebKit, como usado no Google Chrome antes de 7.0.517.44, webkitgtk antes de 1.2.6 e outros produtos, não manipula corretamente grandes áreas de texto, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente outro impacto não especificado através de um documento HTML criado.
CVE-2010-4197	A vulnerabilidade "use-after-free" no WebKit, usada no Google Chrome antes de 7.0.517.44, webkitgtk antes de 1.2.6, e outros produtos, permite que atacantes remotos causem uma negação de serviço ou tenham outro impacto não especificado através de vetores envolvendo edição de texto.
CVE-2010-4042	O Google Chrome anterior à versão 7.0.517.41 não manipula corretamente os mapas de elementos, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a "elementos obsoletos".
CVE-2010-4041	A implementação do sandbox no Google Chrome antes do 7.0.517.41 no Linux não restringe adequadamente os processos de trabalho, o que pode permitir que atacantes remotos contornem as restrições de acesso pretendidas por meio de vetores não especificados.
CVE-2010-4040	O Google Chrome anterior à versão 7.0.517.41 não lida adequadamente com imagens GIF animadas, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de uma imagem criada.
CVE-2010-4039	O Google Chrome anterior ao 7.0.517.41 no Linux não define corretamente a variável de ambiente PATH, que possui vetores de impacto e de ataque não especificados.
CVE-2010-4038	A implementação de Web Sockets no Google Chrome anterior a 7.0.517.41 não lida corretamente com uma ação de desligamento, o que permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2010-4037	A vulnerabilidade não especificada no Google Chrome anterior a 7.0.517.41 permite que invasores remotos ignorem o bloqueador de pop-up por meio de vetores desconhecidos.
CVE-2010-4036	O Google Chrome anterior à versão 7.0.517.41 não lida corretamente com o descarregamento de uma página, o que permite que invasores remotos falsifiquem URLs por meio de vetores não especificados.
CVE-2010-4035	O Google Chrome anterior à versão 7.0.517.41 não executa corretamente as operações de preenchimento automático de formulários, o que permite que invasores remotos causem uma

Nome	Descrição
	negação de serviço (falha do aplicativo) ou possivelmente tenham outro impacto não especificado por meio de um documento HTML criado.
CVE-2010-4034	O Google Chrome, antes do 7.0.517.41, não manipula corretamente os formulários, o que permite que invasores remotos causem uma negação de serviço (falha do aplicativo) ou, possivelmente, tenham outro impacto não especificado por meio de um documento HTML criado.
CVE-2010-4033	O Google Chrome anterior à versão 7.0.517.41 não implementa adequadamente a funcionalidade de preenchimento automático e preenchimento automático, o que permite que atacantes remotos realizem ataques de "perfil de spam" por meio de vetores não especificados.
CVE-2010-4008	libxml2 antes de 2.7.8, conforme usado no Google Chrome antes de 7.0.517.44, o Apple Safari 5.0.2 e anteriores, e outros produtos, lêem de locais de memória inválidos durante o processamento de expressões XPath malformadas, o que permite que invasores dependentes do contexto causem uma negação de serviço (falha de aplicativo) por meio de um documento XML criado.
CVE-2010-3730	O Google Chrome anterior à versão 6.0.472.62 não usa corretamente informações sobre a origem de um documento para gerenciar propriedades, o que permite que invasores remotos tenham um impacto não especificado por meio de um site criado, relacionado a um problema de "poluição de propriedade".
CVE-2010-3729	A implementação do protocolo SPDY no Google Chrome anterior à 6.0.472.62 não gerencia adequadamente os buffers, o que pode permitir que atacantes remotos executem código arbitrário por meio de vetores não especificados.
CVE-2010-3417	O Google Chrome anterior à versão 6.0.472.59 não solicita ao usuário antes de conceder acesso ao histórico de extensão, o que permite que os invasores obtenham informações potencialmente confidenciais por meio de vetores não especificados.
CVE-2010-3416	O Google Chrome antes do 6.0.472.59 no Linux não implementa corretamente o código do idioma Khmer, que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente não tenham outro impacto por meio de vetores desconhecidos.
CVE-2010-3415	O Google Chrome anterior à versão 6.0.472.59 não implementa adequadamente a localização geográfica, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou, possivelmente, não tenham especificado outro impacto por meio de vetores desconhecidos.
CVE-2010-3414	O Google Chrome anterior a 6.0.472.59 no Mac OS X não implementa adequadamente as caixas de diálogo de arquivos, o que permite que os invasores causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto

Nome	Descrição
CVE-2010-3413	não especificado por meio de vetores desconhecidos. Observação: esse problema existe devido a uma correção incorreta para CVE-2010-3112 no Mac OS X.
CVE-2010-3412	A vulnerabilidade não especificada na funcionalidade de bloqueio de pop-up no Google Chrome anterior à 6.0.472.59 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de vetores desconhecidos.
CVE-2010-3411	A condição de corrida na implementação do console no Google Chrome anterior a 6.0.472.59 tem vetores de impacto e ataque não especificados.
CVE-2010-3259	O Google Chrome anterior ao 6.0.472.59 no Linux não lida corretamente com cursores, o que pode permitir que invasores causem uma negação de serviço (falha de asserção) por meio de vetores não especificados.
CVE-2010-3258	O WebKit, como usado no Apple Safari antes de 4.1.3 e 5.0.x antes de 5.0.3, o Google Chrome anterior a 6.0.472.53 e o webkitgtk anterior a 1.2.6, não restringe adequadamente o acesso de leitura a imagens derivadas de elementos CANVAS, o que permite acesso remoto invasores ignorem a Política de mesma origem e obtenham dados de imagem potencialmente confidenciais por meio de um site criado.
CVE-2010-3257	A implementação do sandbox no Google Chrome anterior a 6.0.472.53 não desserializa corretamente os parâmetros, que têm vetores de impacto e ataque remoto não especificados.
CVE-2010-3256	A vulnerabilidade de usar o after-free no WebKit, usada no Apple Safari antes de 4.1.3 e 5.0.x antes de 5.0.3, Google Chrome antes de 6.0.472.53 e webkitgtk antes de 1.2.6, permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (falha do aplicativo) por meio de vetores envolvendo o foco do elemento.
CVE-2010-3255	O Google Chrome anterior à versão 6.0.472.53 não limita adequadamente o número de entradas de preenchimento automático armazenadas, que tem um impacto não especificado e vetores de ataque.
CVE-2010-3254	O Google Chrome anterior a 6.0.472.53 e o webkitgtk anteriores a 1.2.6 não manipulam adequadamente os nós de contador, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3253	A implementação de WebSockets no Google Chrome anterior a 6.0.472.53 não lida corretamente com valores inteiros, o que permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3252	A implementação de permissões de notificação no Google Chrome antes da versão 6.0.472.53 permite que invasores causem uma negação de serviço (corrupção de memória) ou possivelmente

Nome	Descrição
	tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3252	A vulnerabilidade "usar após liberar" no apresentador "Notificações" do Google Chrome antes da versão 6.0.472.53 permite que invasores causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3251	A implementação de WebSockets no Google Chrome anterior a 6.0.472.53 permite que atacantes remotos causem uma negação de serviço (desreferenciamento de ponteiro NULL e falha de aplicativo) por meio de vetores não especificados.
CVE-2010-3250	A vulnerabilidade não especificada no Google Chrome anterior a 6.0.472.53 permite que atacantes remotos enumeram o conjunto de extensões instaladas por meio de vetores desconhecidos.
CVE-2010-3249	O Google Chrome anterior à versão 6.0.472.53 não implementa corretamente os filtros SVG, o que permite que invasores remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos, relacionados a um problema de "ponteiro antigo".
CVE-2010-3248	O Google Chrome anterior à versão 6.0.472.53 não restringe adequadamente a cópia para a área de transferência, que possui vetores de impacto e ataque não especificados.
CVE-2010-3247	O Google Chrome anterior a 6.0.472.53 não restringe adequadamente os caracteres em URLs, o que permite que atacantes remotos falsifiquem a aparência da barra de URL por meio de sequências homográficas.
CVE-2010-3246	O Google Chrome anterior a 6.0.472.53 não manipula adequadamente o valor _blank para o atributo de destino de elementos não especificados, o que permite que atacantes remotos ignorem o bloqueador de pop-ups por meio de vetores desconhecidos.
CVE-2010-3120	O Google Chrome anterior a 5.0.375.127 não implementa adequadamente o recurso de geolocalização, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3119	O Google Chrome anterior a 5.0.375.127 e o webkitgtk anteriores a 1.2.6 não suportam adequadamente a linguagem Ruby, o que permite que os atacantes causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado através de vetores desconhecidos.
CVE-2010-3118	O recurso de sugestão automática na implementação da omnibox no Google Chrome anterior a 5.0.375.127 não prevê a entrada de senhas, o que pode permitir que atacantes remotos obtenham informações confidenciais lendo o tráfego de rede gerado por esse recurso.

Nome	Descrição
CVE-2010-3117	O Google Chrome anterior a 5.0.375.127 não implementa adequadamente o recurso de notificações, o que permite que atacantes remotos causem uma negação de serviço (falha no aplicativo) e possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3116	Várias vulnerabilidades de uso após a liberação no WebKit, como usadas no Apple Safari anteriores a 4.1.3 e 5.0.x antes de 5.0.3, Google Chrome antes de 5.0.375.127 e webkitgtk antes de 1.2.6, permitem que atacantes remotos executem código arbitrário ou causar uma negação de serviço (falha do aplicativo) por meio de vetores relacionados ao manuseio inadequado de tipos MIME por plug-ins.
CVE-2010-3115	O Google Chrome anterior a 5.0.375.127 e o webkitgtk anterior à 1.2.6 não implementam adequadamente o recurso de histórico, o que pode permitir que invasores remotos falsifiquem a barra de endereço por meio de vetores não especificados.
CVE-2010-3114	A implementação de edição de texto no Google Chrome anterior a 5.0.375.127 e webkitgtk antes da versão 1.2.6 não verifica um tipo de nó antes de realizar um lançamento, que tem um impacto não especificado e vetores de ataque relacionados a (1) DeleteSelectionCommand.cpp, (2) InsertLineBreakCommand.cpp ou (3) InsertParagraphSeparatorCommand.cpp no WebCore / editing /.
CVE-2010-3113	O Google Chrome anterior a 5.0.375.127 e o webkitgtk antes do 1.2.5 não manipulam adequadamente documentos SVG, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos relacionados a alterações de estado DeleteButtonController.
CVE-2010-3112	O Google Chrome anterior a 5.0.375.127 não implementa adequadamente as caixas de diálogo de arquivos, o que permite que os invasores causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-3111	O Google Chrome anterior à versão 6.0.472.53 não atenua adequadamente uma falha não especificada no kernel do Windows, que tem impacto e vetores de ataque desconhecidos, uma vulnerabilidade diferente da CVE-2010-2897.
CVE-2010-2903	O Google Chrome anterior a 5.0.375.125 realiza o truncamento inesperado e o cancelamento indevido de nomes de host, que possui vetores de impacto e ataque remoto não especificados.
CVE-2010-2902	A implementação de SVG no Google Chrome anterior a 5.0.375.125 permite que invasores remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-2901	A implementação de renderização no Google Chrome anterior a 5.0.375.125 permite que atacantes remotos causem uma negação

Nome	Descrição
	de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-2900	O Google Chrome anterior a 5.0.375.125 não manipula adequadamente uma tela grande, que possui vetores de impacto e ataque remoto não especificados.
CVE-2010-2899	A vulnerabilidade não especificada na implementação de layout no Google Chrome anterior a 5.0.375.125 permite que atacantes remotos obtenham informações confidenciais da memória de processo por meio de vetores desconhecidos.
CVE-2010-2898	O Google Chrome anterior a 5.0.375.125 não atenua adequadamente uma falha não especificada na Biblioteca C GNU, que tem impacto e vetores de ataque desconhecidos.
CVE-2010-2897	O Google Chrome anterior a 5.0.375.125 não atenua adequadamente uma falha não especificada no kernel do Windows, que tem impacto e vetores de ataque desconhecidos.
CVE-2010-2652	O Google Chrome anterior à versão 5.0.375.99 não implementa adequadamente as caixas de diálogo modais, o que permite que os invasores causem uma negação de serviço (falha do aplicativo) por meio de vetores não especificados.
CVE-2010-2651	A implementação CSS (Cascading Style Sheets) no Google Chrome anterior a 5.0.375.99 não executa corretamente a renderização de estilo, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-2650	A vulnerabilidade não especificada no Google Chrome anterior a 5.0.375.99 tem impacto e vetores de ataque desconhecidos, relacionados a um "incômodo com diálogos de impressão".
CVE-2010-2649	A vulnerabilidade não especificada no Google Chrome anterior à 5.0.375.99 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de uma imagem inválida.
CVE-2010-2648	A implementação do Algoritmo Bidirecional Unicode (também conhecido como algoritmo Bidi ou UBA) no Google Chrome antes de 5.0.375.99 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-2647	O Google Chrome anterior à 5.0.375.99 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente tenham outro impacto não especificado por meio de um documento SVG inválido.
CVE-2010-2646	O Google Chrome anterior à 5.0.375.99 não isola adequadamente elementos IFRAME em área restrita, que possui vetores de impacto e ataque remoto não especificados.
CVE-2010-2645	A vulnerabilidade não especificada no Google Chrome anterior a 5.0.375.99, quando o WebGL é usado, permite que atacantes remotos causem uma negação de serviço (leitura fora dos limites)

Nome	Descrição
	por meio de vetores desconhecidos.
CVE-2010-2302	A vulnerabilidade use-after-free no WebCore no WebKit no Google Chrome antes de 5.0.375.70 permite que atacantes remotos causem uma negação de serviço (corrupção de memória) ou possivelmente executem código arbitrário por meio de vetores envolvendo fontes remotas em conjunto com árvores DOM de sombra, também conhecido como rdar problema 8007953. NOTA: isso pode se sobrepor ao CVE-2010-1771.
CVE-2010-2301	A vulnerabilidade de cross-site scripting (XSS) na edição / markup.cpp no WebCore no WebKit no Google Chrome anterior a 5.0.375.70 permite que invasores remotos injetem script web ou HTML arbitrário por meio de vetores relacionados à propriedade node.innerHTML de um elemento TEXTAREA.NOTA: isso pode se sobrepor ao CVE-2010-1762.
CVE-2010-2300	A vulnerabilidade use-after-free na função Element :: normalizeAttributes em dom / Element.cpp no WebCore no WebKit no Google Chrome antes de 5.0.375.70 permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória) por meio de vetores relacionados para manipuladores de eventos de mutação DOM, também conhecido como rdar problema 7948784. NOTA: isso pode se sobrepor CVE-2010-1759.
CVE-2010-2299	A função Clipboard :: DispatchObject em app / clipboard / clipboard.cc no Google Chrome antes de 5.0.375.70 não manipula corretamente objetos CBF_SMBITMAP em uma mensagem ViewHostMsg_ClipboardWriteObjectsAsync, que pode permitir que atacantes remotos executem código arbitrário por meio de vetores envolvendo dados criados do processo renderizador , relacionado a um problema de "Confusão de tipos".
CVE-2010-2298	browser / renderer_host / database_dispatcher_host.cc no Google Chrome antes de 5.0.375.70 no Linux não manipula corretamente as mensagens ViewHostMsg_DatabaseOpenFile no sandboxing baseado em chroot, que permite que atacantes remotos contornem as restrições de sandbox desejadas por meio de vetores envolvendo chamadas fchdir e chdir.
CVE-2010-2297	rendering / FixedTableLayout.cpp no WebCore no WebKit no Google Chrome antes de 5.0.375.70 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente executar código arbitrário através de um documento HTML que tenha um grande atributo colspan dentro de uma tabela.
CVE-2010-2296	A implementação de métodos DOM não especificados no Google Chrome anteriores a 5.0.375.70 permite que invasores remotos contornem a Política de mesma origem por meio de vetores desconhecidos.
CVE-2010-2295	O page / EventHandler.cpp no WebCore no WebKit no Google Chrome anterior à 5.0.375.70 não manipula adequadamente uma alteração do quadro focalizado durante o despacho do keydown,

Nome	Descrição
	que permite que atacantes remotos assistidos por usuário redirecionem as teclas digitadas por meio de um documento HTML criado, também conhecido como rdar problema 7018610. NOTA: isso pode se sobrepor ao CVE-2010-1422.
CVE-2010-2120	O Google Chrome 1.0.154.48 permite que atacantes remotos causem uma negação de serviço (consumo de recursos) por meio do código JavaScript que contém um loop infinito que cria elementos IFRADE para notícias inválidas: // URIs.
CVE-2010-2110	O Google Chrome anterior à 5.0.375.55 não executa corretamente o código JavaScript no contexto da extensão, que possui vetores de impacto e ataque remoto não especificados.
CVE-2010-2109	A vulnerabilidade não especificada no Google Chrome anterior a 5.0.375.55 permite que invasores remotos assistidos por usuários causem uma negação de serviço (erro de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à funcionalidade "arrastar e soltar".
CVE-2010-2108	A vulnerabilidade não especificada no Google Chrome anterior a 5.0.375.55 permite que invasores remotos ignorem o bloqueador de plug-ins de modo de lista de permissões por meio de vetores desconhecidos.
CVE-2010-2107	A vulnerabilidade não especificada no Google Chrome anterior a 5.0.375.55 permite que os invasores causem uma negação de serviço (erro de memória) ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados à funcionalidade de Navegação segura.
CVE-2010-2106	A vulnerabilidade não especificada no Google Chrome anterior a 5.0.375.55 pode permitir que invasores remotos falsifiquem a barra de URL por meio de vetores que envolvam o descarregamento de manipuladores de eventos.
CVE-2010-2105	O Google Chrome anterior a 5.0.375.55 não segue adequadamente os requisitos da especificação de Navegação segura para canonização de URLs, que possui vetores de impacto e ataque remoto não especificados.
CVE-2010-1992	O Google Chrome 1.0.154.48 executa um aplicativo de email em situações em que um elemento IFRADE possui uma URL mailto: URL em seu atributo SRC, que permite que atacantes remotos causem uma negação de serviço (inicialização excessiva de aplicativos) por meio de um documento HTML com muitos elementos IFRADE.
CVE-2010-1851	O Google Chrome, quando a extensão Invisible Hand está ativada, usa cookies durante as solicitações HTTP de fundo de uma maneira possivelmente inesperada, o que pode permitir que servidores remotos identifiquem pessoas específicas e suas pesquisas de produtos por meio de registro de solicitações HTTP, relacionadas a "dados entre sites vazamento "questão.
CVE-2010-1825	A vulnerabilidade use-after-free no WebKit, como usada no Google Chrome antes da versão 6.0.472.59, permite que atacantes

Nome	Descrição
	remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado por meio de vetores relacionados a elementos SVG aninhados.
CVE-2010-1824	A vulnerabilidade "use-after-free" no WebKit, usada no Apple iTunes antes do 10.2 no Windows, Apple Safari e Google Chrome antes do 6.0.472.59, permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço através de vetores relacionados a estilos SVG, a árvore DOM e as mensagens de erro.
CVE-2010-1823	A vulnerabilidade use-after-free no WebKit antes de r65958, como usada no Google Chrome antes de 6.0.472.59, permite que atacantes remotos causem uma negação de serviço ou possivelmente tenham outro impacto não especificado via vetores que acionam o uso de APIs de documentos, como document.close durante análise, como demonstrado por um arquivo Cascading Style Sheets (CSS) referenciando uma fonte SVG inválida, também conhecida como rdar problema 8442098.
CVE-2010-1822	O WebKit, como usado no Apple Safari antes do 4.1.3 e 5.0.x antes do 5.0.3 e do Google Chrome antes do 6.0.472.62, não executa adequadamente uma conversão de uma variável não especificada, que permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (falha de aplicativo) por meio de um elemento SVG em um documento não-SVG.
CVE-2010-1773	O erro off-by-one na função toAlphabetic no render / RenderListMarker.cpp no WebCore no WebKit antes do r59950, como usado no Google Chrome antes de 5.0.375.70, permite que atacantes remotos obtenham informações confidenciais, causem uma negação de serviço (corrupção de memória e falha de aplicativo), ou possivelmente executar código arbitrário por meio de vetores relacionados a marcadores de lista para listas HTML, também conhecido como rdar problem 8009118.
CVE-2010-1772	A vulnerabilidade use-after-free na página / Geolocation.cpp no WebCore no WebKit antes do r59859, como usada no Google Chrome antes de 5.0.375.70, permite que atacantes remotos executem código arbitrário ou causem uma negação de serviço (falha do aplicativo) por meio de uma Web trabalhada site, relacionado à falha em interromper temporizadores associados à geolocalização após a exclusão de um documento.
CVE-2010-1770	O WebKit no Apple Safari anterior a 5.0 no Mac OS X 10.5 a 10.6 e Windows, o Apple Safari antes de 4.1 no Mac OS X 10.4 e o Google Chrome anterior a 5.0.375.70 não manipula adequadamente uma transformação de um nó de texto que possui o conjunto de caracteres IBM1147 que permite que invasores remotos executem código arbitrário ou causem uma negação de serviço (corrupção de memória e falha de aplicativo) por meio de um documento HTML criado contendo um elemento BR, relacionado a um "problema de verificação de tipo".
CVE-2010-1767	A vulnerabilidade de falsificação de solicitação entre sites (CSRF)

Nome	Descrição
	no carregador / DocumentThreadableLoader.cpp no WebCore no WebKit antes do r57041, usada no Google Chrome anterior a 4.1.249.1059, permite que invasores remotos sequurem a autenticação de vítimas não especificadas por meio de uma operação XMLHttpRequest de pré-visualização síncrona.
CVE-2010-1731	O Google Chrome no HTC Hero permite que atacantes remotos causem uma negação de serviço (falha de aplicativo) via JavaScript que grava seqüências <marquee> em um loop infinito.
CVE-2010-1665	O Google Chrome anterior a 4.1.249.1064 não processa corretamente as fontes, o que permite que invasores remotos causem uma negação de serviço (corrupção de memória) e possivelmente tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-1664	O Google Chrome anterior a 4.1.249.1064 não lida corretamente com mídia HTML5, o que permite que atacantes remotos causem uma negação de serviço (corrupção de memória) e, possivelmente, tenham outro impacto não especificado por meio de vetores desconhecidos.
CVE-2010-1663	A Biblioteca de análise de URLs do Google (também conhecida como google-url ou GURL) no Google Chrome anterior a 4.1.249.1064 permite que invasores remotos ignorem a Política de mesma origem por meio de vetores não especificados.
CVE-2010-1506	As ligações do Google V8 no Google Chrome anteriores a 4.1.249.1059 permitem que os invasores causem uma negação de serviço (corrupção de memória) por meio de vetores desconhecidos.
CVE-2010-1505	O Google Chrome anterior a 4.1.249.1059 não impede que páginas sejam carregadas com os privilégios da página "Nova guia", que tem impacto e vetores de ataque desconhecidos.
CVE-2010-1504	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome anterior a 4.1.249.1059 permite que invasores remotos injetem scripts da Web ou HTML arbitrários por meio de vetores relacionados a um URI chrome: // downloads.
CVE-2010-1503	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome anterior a 4.1.249.1059 permite que invasores remotos injetem scripts da Web ou HTML arbitrários por meio de vetores relacionados a um URI chrome: // net-internals.
CVE-2010-1502	A vulnerabilidade não especificada no Google Chrome anterior a 4.1.249.1059 permite que atacantes remotos acessem arquivos locais por meio de vetores relacionados a "ferramentas do desenvolvedor".
CVE-2010-1500	O Google Chrome anterior a 4.1.249.1059 não oferece suporte a formulários, que têm impacto e vetores de ataque desconhecidos, relacionados a um "erro de confusão de tipo".
CVE-2010-1237	O Google Chrome 4.1 BETA anterior a 4.1.249.1036 permite que atacantes remotos causem uma negação de serviço (erro de

Nome	Descrição
	memória) ou possivelmente tenham outro impacto não especificado por meio de um elemento SVG vazio.
CVE-2010-1236	O protocolo Is funciona na plataforma / KURLGoogle.cpp no WebCore no WebKit antes de o r55822, conforme usado no Google Chrome antes de 4.1.249.1036 e no Flock Browser 3.x antes de 3.0.0.4112, não manipular corretamente os espaços em branco no início de um URL, o que permite invasores remotos para conduzir ataques de cross-site scripting (XSS) por meio de um javascript: URL, conforme demonstrado por uma sequência de alertas \x00javascript:.
CVE-2010-1235	A vulnerabilidade não especificada no Google Chrome anterior a 4.1.249.1036 permite que atacantes remotosacionem a omissão de um diálogo de aviso de download por meio de vetores desconhecidos.
CVE-2010-1234	A vulnerabilidade não especificada no Google Chrome anterior a 4.1.249.1036 permite que invasores remotos truncem a URL mostrada na caixa de diálogo Autenticação básica HTTP por meio de vetores desconhecidos.
CVE-2010-1233	Vários transbordos de números inteiros no Google Chrome anteriores a 4.1.249.1036 permitem que invasores remotos tenham um impacto não especificado por meio de vetores envolvendo objetos JavaScript do WebKit.
CVE-2010-1232	O Google Chrome anterior a 4.1.249.1036 permite que invasores remotos causem uma negação de serviço (erro de memória) ou possivelmente não tenham outro impacto não especificado por meio de um documento SVG malformado.
CVE-2010-1231	O Google Chrome anterior a 4.1.249.1036 processa os cabeçalhos HTTP antes de invocar o recurso SafeBrowsing, que permite que invasores remotos tenham um impacto não especificado por meio de cabeçalhos criados.
CVE-2010-1230	O Google Chrome anterior a 4.1.249.1036 não possui o comportamento esperado para tentativas de excluir bancos de dados SQL da Web e limpar o estado de segurança de transporte restrita (STS), que possui vetores de impacto e de ataque não especificados.
CVE-2010-1229	A infraestrutura do sandbox no Google Chrome anterior a 4.1.249.1036 não usa corretamente ponteiros, que possuem vetores de impacto e ataque não especificados.
CVE-2010-1228	Várias condições de corrida na infraestrutura do sandbox no Google Chrome anteriores a 4.1.249.1036 têm vetores de impacto e ataque não especificados.
CVE-2010-1126	A implementação do JavaScript no WebKit permite que atacantes remotosenviem pressionamentos de tecla selecionados para um campo de formulário em um quadro oculto, em vez do campo de formulário pretendido em um quadro visível, por meio de determinadas chamadas para o método de foco.

Nome	Descrição
CVE-2010-1029	A vulnerabilidade do consumo de pilha na função WebCore :: CSSSelector no WebKit, como usada no Apple Safari 4.0.4, no Apple Safari no iPhone OS e no iPhone OS para o iPod touch, e no Google Chrome 4.0.249, permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente executar código arbitrário por meio de um elemento STYLE composto por um grande número de sequências *>.
CVE-2010-0664	A vulnerabilidade do consumo de pilha na função ChildProcessSecurityPolicy :: CanRequestURL no navegador / child_process_security_policy.cc no Google Chrome anterior a 4.0.249.78 permite que invasores remotos causem uma negação de serviço (consumo de memória e falha de aplicativo) por meio de uma URL que especifica vários protocolos, conforme demonstrado um URL que começa com muitas repetições da fonte de exibição: substring.
CVE-2010-0663	A função ParamTraits <SkBitmap> :: Read em common / common_param_traits.cc no Google Chrome anterior a 4.0.249.78 não inicializa os locais de memória que armazenam dados de bitmap, o que pode permitir que atacantes remotos obtenham informações potencialmente confidenciais da memória de processo, fornecendo informações insuficientes dados, relacionados ao uso de um (1) banco de dados de miniaturas ou (2) tela HTML.
CVE-2010-0662	A função ParamTraits <SkBitmap> :: Read em common / common_param_traits.cc no Google Chrome anterior a 4.0.249.78 não usa as variáveis corretas em cálculos projetados para evitar transbordamentos de inteiros, o que permite que invasores aproveitem o acesso do renderizador para causar uma negação de serviço ou possivelmente não tenha especificado outro impacto através de dados de bitmap, relacionados à desserialização.
CVE-2010-0661	WebCore / bindings / v8 / custom / V8DOMWindowCustom.cpp no WebKit antes de r52401, conforme usado no Google Chrome antes de 4.0.249.78, permite que atacantes remotos contornem a Política de mesma origem por meio de vetores que envolvam o método window.open.
CVE-2010-0660	O Google Chrome anterior a 4.0.249.78 envia uma URL https no cabeçalho Referer de uma solicitação http em determinadas circunstâncias, envolvendo o redirecionamento https para http, que permite que os servidores HTTP remotos obtenham informações potencialmente confidenciais por meio do log HTTP padrão.
CVE-2010-0659	O decodificador de imagens do WebKit antes do r52833, usado no Google Chrome antes de 4.0.249.78, não manipula adequadamente uma falha de alocação de memória, que permite que atacantes remotos executem código arbitrário na sandbox do Chrome por meio de um arquivo GIF malformado que especifica um tamanho grande .
CVE-2010-0658	Vários overflows inteiros no Skia, conforme usados no Google Chrome antes de 4.0.249.78, permitem que atacantes remotos executem código arbitrário na sandbox do Chrome ou causem uma

Nome	Descrição
CVE-2010-0657	negação de serviço (corrupção de memória e falha de aplicativo) por meio de vetores envolvendo elementos CANVAS.
CVE-2010-0656	O Google Chrome anterior a 4.0.249.78 no Windows não executa a codificação, o escape e a cotação esperados para o URL no argumento --app em um atalho na área de trabalho, que permite que atacantes remotos assistidos por usuário executem programas arbitrários ou obtenham informações confidenciais ao enganar um usuário para criar um atalho criado.
CVE-2010-0656	O WebKit antes do r51295, usado no Google Chrome antes de 4.0.249.78, apresenta uma página de listagem de diretório em resposta a um XMLHttpRequest para um arquivo: /// URL que corresponde a um diretório, que permite que invasores obtenham informações confidenciais ou possivelmente não especificadas outro impacto por meio de um documento HTML local criado.
CVE-2010-0655	A vulnerabilidade "usar-depois-livre" no Google Chrome anterior a 4.0.249.78 permite que invasores remotos assistidos por usuário causem uma negação de serviço (falha do aplicativo) ou possivelmente executar código arbitrário por meio de vetores que envolvam a exibição de uma janela pop-up bloqueada durante a navegação para uma Web diferente local.
CVE-2010-0651	O WebKit antes do r52784, usado no Google Chrome antes do 4.0.249.78 e no Apple Safari antes do 4.0.5, permite o carregamento entre origens de folhas de estilos CSS mesmo quando o download da folha de estilo tem um tipo MIME incorreto e o documento da folha de estilo está malformado, o que permite ataques remotos para obter informações confidenciais através de um documento elaborado.
CVE-2010-0650	O WebKit, como usado no Google Chrome antes de 4.0.249.78 e no Apple Safari, permite que atacantes remotos contornem as restrições previstas em janelas pop-up através do uso de um evento de clique do mouse.
CVE-2010-0649	O estouro de número inteiro na função CrossCallParamsEx :: CreateFromBuffer em sandbox / src / crosscall_server.cc no Google Chrome antes de 4.0.249.89 permite que invasores aproveitem o acesso do renderizador para causar uma negação de serviço (corrupção de memória de heap) ou possivelmente ter outro impacto não especificado por meio de um malformado mensagem, relacionada à desserialização de mensagens do sandbox.
CVE-2010-0647	O WebKit antes do r53525, usado no Google Chrome antes de 4.0.249.89, permite que atacantes remotos executem código arbitrário na sandbox do Chrome por meio de um elemento RUBY malformado, conforme demonstrado por uma sequência <ruby><table><rt>.
CVE-2010-0646	Vários erros de assinatura de números inteiros em factory.cc no Google V8 anteriores a r3560, conforme usados no Google Chrome antes de 4.0.249.89, permitem que atacantes remotos executem código arbitrário na sandbox do Google Chrome por meio do uso de

Nome	Descrição
matrizes JavaScript.	matrizes JavaScript.
CVE-2010-0645	Vários overflows inteiros no factory.cc no Google V8 anteriores ao r3560, conforme usados no Google Chrome antes de 4.0.249.89, permitem que atacantes remotos executem código arbitrário na sandbox do Google Chrome por meio do uso de matrizes JavaScript.
CVE-2010-0644	O Google Chrome anterior a 4.0.249.89, quando um servidor proxy SOCKS 5 é configurado, envia consultas DNS diretamente, o que permite que servidores DNS remotos obtenham informações potencialmente confidenciais sobre a identidade de um usuário cliente por meio de registro de solicitações, conforme demonstrado por um servidor proxy configurado para fins de anonimato.
CVE-2010-0643	O Google Chrome anterior a 4.0.249.89 tenta estabelecer conexões diretas com sites da Web quando todos os servidores proxy configurados não estão disponíveis, o que permite que servidores HTTP remotos obtenham informações potencialmente confidenciais sobre a identidade de um usuário cliente via registro HTTP padrão, conforme demonstrado por um servidor proxy que foi configurado com o propósito de anonimato.
CVE-2010-0556	browser / login / login_prompt.cc no Google Chrome antes de 4.0.249.89 preenche um diálogo de autenticação com credenciais que foram armazenadas pelo Password Manager para um site diferente, que permite que servidores HTTP remotos assistidos por usuário obtenham informações confidenciais por meio de um URL que requer autenticação , conforme demonstrado por um URL no atributo SRC de um elemento IMG.
CVE-2010-0315	O WebKit anterior ao r53607, usado no Google Chrome antes de 4.0.249.89, permite que atacantes remotos descubram o URL de destino de um redirecionamento, para a sessão de um usuário específico de um site, colocando o URL do site no atributo HREF de um elemento LINK de folha de estilo e, em seguida, ler o valor da propriedade document.styleSheets [0] .href, relacionado a um elemento IFRAME.
CVE-2009-3934	A função WebFrameLoaderClient :: dispatchDidChangeLocationWithinPage em src / webkit / glue / webframeclient_impl.cc no Google Chrome anterior a 3.0.195.32 permite que invasores remotos assistidos por usuário causem uma negação de serviço por meio de um link de página local, relacionado a uma "cadeia de redirecionamento vazia". "como demonstrado por uma mensagem no Yahoo! Enviar.
CVE-2009-3933	O WebKit anterior ao r50173, usado no Google Chrome antes de 3.0.195.32, permite que atacantes remotos causem uma negação de serviço (consumo de CPU) por meio de uma página da web que chama o método setInterval do JavaScript, que dispara uma incompatibilidade entre o WTF :: currentTime e :: funções do tempo.
CVE-2009-3932	O plug-in Gears no Google Chrome anterior a 3.0.195.32 permite

Nome	Descrição
CVE-2009-3931	que invasores remotos assistidos por usuários causem uma negação de serviço (corrupção de memória e falha no plug-in) ou possivelmente executar código arbitrário por meio de uso não especificado da API do Gears SQL relacionada a "metadados SQL" um estado ruim .
CVE-2009-3456	A vulnerabilidade incompleta da lista negra no navegador / download / download_exe.cc no Google Chrome anterior a 3.0.195.32 permite que invasores remotos forcem o download de determinados arquivos perigosos por meio de uma designação "Content-Disposition: attachment", conforme demonstrado por (1) .mht e (2) arquivos .mhtml, que são executados automaticamente pelo Internet Explorer 6; (3) arquivos .svg, que são executados automaticamente pelo Safari; (4) arquivos .xml; (5) arquivos .htt; (6) arquivos .xsl; (7) arquivos .xslt; e (8) arquivos de imagem que são proibidos pela política do site da vítima.
CVE-2009-3270	O Google Chrome, possivelmente 3.0.195.21 e anterior, não manipula adequadamente um caractere '\ 0' em um nome de domínio no campo Common Name (CN) do assunto de um certificado X.509, o que permite que os invasores man-in-the-middle para falsificar servidores SSL arbitrários por meio de um certificado criado por uma autoridade de certificação legítima, um problema relacionado ao CVE-2009-2408. NOTA: a procedência desta informação é desconhecida; os detalhes são obtidos exclusivamente de informações de terceiros.
CVE-2009-3269	O Microsoft Internet Explorer 7 a 7.0.6000.16711 permite que atacantes remotos causem uma negação de serviço (navegador inutilizável) chamando a função window.print em um loop, também conhecido como "imprimindo ataque DoS", possivelmente um problema relacionado ao CVE-2009-0821 .
CVE-2009-3268	O Opera 9.52 e anteriores permitem que atacantes remotos causem uma negação de serviço (consumo de CPU) através de uma série de envios automáticos de um formulário contendo um elemento KEYGEN, um problema relacionado ao CVE-2009-1828.
CVE-2009-3267	O Google Chrome 1.0.154.48 e anterior permite que invasores remotos causem uma negação de serviço (consumo de CPU) por meio de um formulário enviado automaticamente contendo um elemento KEYGEN, um problema relacionado ao CVE-2009-1828.
CVE-2009-3264	O Microsoft Internet Explorer 6 a 6.0.2900.2180 e 7.0.6000.16711 permite que atacantes remotos causem uma negação de serviço (consumo de CPU) por meio de um formulário enviado automaticamente contendo um elemento KEYGEN, um problema relacionado ao CVE-2009-1828.
	O método getSVGDocument no Google Chrome anterior a 3.0.195.21 omite uma "verificação de acesso" não especificada, que permite que servidores remotos ignorem a Política de mesma origem e conduzam ataques de script entre sites por meio de vetores desconhecidos, relacionados à visita de um usuário a um servidor da Web diferente que hospeda um documento SVG.

Nome	Descrição
CVE-2009-3263	A vulnerabilidade de cross-site scripting (XSS) no Google Chrome 2.xe 3.x antes do 3.0.195.21 permite que invasores remotos injetem scripts web ou HTML arbitrários por meio de um (1) RSS ou (2) feed Atom, relacionado à renderização de o tipo de conteúdo application / rss + xml como XML "active content".
CVE-2009-3011	O Google Chrome 1.0.154.48 e anteriores, 2.0.172.28, 2.0.172.37 e 3.0.193.2 Beta não bloqueia dados adequadamente: URIs em Atualizar cabeçalhos em respostas HTTP, o que permite que atacantes remotos conduzam ataques de cross-site scripting (XSS) via vectores relacionados com (1) injectar um cabeçalho Refresh que contenha sequências JavaScript num dado: text / html URI ou (2) introduzir um URI data: text / html com sequências JavaScript ao especificar o conteúdo de um cabeçalho Refresh. NOTA: o JavaScript é executado fora do contexto do site HTTP.
CVE-2009-2975	O Mozilla Firefox 3.5.2 no Windows XP, em algumas situações possivelmente envolvendo um manipulador de protocolo configurado incompletamente, não implementa adequadamente a configuração da propriedade document.location para um valor que especifica um protocolo associado a um aplicativo externo, que permite que atacantes remotos causem uma negação de serviço (consumo de memória) através de vetores envolvendo uma série de chamadas de função que definem esta propriedade, como demonstrado por (1) o protocolo chromehtml: e (2) o objetivo: protocolo.
CVE-2009-2974	O Google Chrome 1.0.154.65, 1.0.154.48 e anterior permite que atacantes remotos (1) causem uma negação de serviço (interrupção do aplicativo) por meio de vetores envolvendo um valor chromehtml: URI para a propriedade document.location ou (2) causem uma negação de serviço (bloqueio de aplicativo e consumo de CPU) por meio de vetores envolvendo uma série de chamadas de função que definem um valor de chromehtml: URI para a propriedade document.location.
CVE-2009-2973	O Google Chrome anterior à versão 2.0.172.43 não impede as ligações SSL a um site com um certificado X.509 assinado com o algoritmo MD2 ou MD4, o que facilita a falsificação arbitrária de invasores man-in-the-middle Servidores HTTPS por meio de um certificado criado, um problema relacionado ao CVE-2009-2409.
CVE-2009-2955	O Google Chrome 1.0.154.48 e anteriores permite que atacantes remotos causem uma negação de serviço (consumo de CPU e interrupção de aplicativo) via código JavaScript com um valor de cadeia longa para a propriedade hash (também conhecida como location.hash), um problema relacionado ao CVE-2008- 5715.
CVE-2009-2935	O Google V8, usado no Google Chrome antes de 2.0.172.43, permite que atacantes remotos contornem as restrições à leitura de memória e, possivelmente, obtenham informações confidenciais ou executem código arbitrário na sandbox do Google Chrome, por meio de JavaScript criado.
CVE-2009-2816	A implementação do CORS (Cross-Origin Resource Sharing) no

Nome	Descrição
CVE-2009-2578	WebKit, usado no Apple Safari antes do 4.0.4 e no Google Chrome antes de 3.0.195.33, inclui determinados cabeçalhos HTTP personalizados na solicitação OPTIONS durante operações de origem cruzada com preflight, o que torna é mais fácil para invasores remotos realizar ataques de falsificação de solicitações entre sites (CSRF) por meio de uma página da Web criada.
CVE-2009-2556	O Google Chrome 2.x até 2.0.172 permite que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de um longo argumento de cadeia Unicode ao método de gravação, um problema relacionado ao CVE-2009-2479.
CVE-2009-2555	O Google Chrome anterior a 2.0.172.37 permite que invasores aproveitem o acesso do renderizador para causar uma negação de serviço (corrupção de memória e falha de aplicativo) ou possivelmente executar código arbitrário por meio de vetores não especificados que acionam a alocação excessiva de memória.
CVE-2009-2352	O estouro de buffer com base em heap em src / jsregexp.cc no Google V8 anterior a 1.1.10.14, conforme usado no Google Chrome anterior a 2.0.172.37, permite que atacantes remotos executem código arbitrário na sandbox do Google Chrome por meio de uma expressão regular JavaScript criada.
CVE-2009-2121	O Google Chrome 1.0.154.48 e anterior não bloqueia javascript: URIs em Atualizar cabeçalhos em respostas HTTP, que permite que atacantes remotos conduzam ataques de cross-site scripting (XSS) por meio de vetores relacionados a (1) injeção de um cabeçalho de atualização ou (2) especificação o conteúdo de um cabeçalho de atualização, um problema relacionado ao CVE-2009-1312. NOTA: foi posteriormente relatado que 2.0.172.28, 2.0.172.37 e 3.0.193.2 Beta também são afetados.
CVE-2009-2071	O estouro de buffer no kernel do navegador no Google Chrome anterior a 2.0.172.33 permite que servidores HTTP remotos causem uma negação de serviço (falha do aplicativo) ou possivelmente executem código arbitrário por meio de uma resposta criada.
CVE-2009-2068	O Google Chrome anterior a 1.0.154.53 exibe um certificado em cache para uma página de resposta (1) 4xx ou (2) 5xx CONNECT retornada por um servidor proxy, que permite que invasores man-in-the-middle falsifiquem um site https arbitrário, permitindo que um navegador obtenha um certificado válido deste site durante uma solicitação e, em seguida, envie ao navegador uma página de resposta 502 criada em uma solicitação subsequente.
	O Google Chrome detecta conteúdo http em https páginas da Web somente quando o quadro de nível superior usa https, o que permite que invasores intermediários executem scripts da web arbitrários, no contexto de um site https, modificando uma página http para incluir um https iframe que faz referência a um arquivo de script em um site http, relacionado a páginas "HTTP-Intended-but-HTTPS-Loadable (HPIHSL)".

Nome	Descrição
CVE-2009-2060	src / net / http / http_transaction_winhttp.cc no Google Chrome antes de 1.0.154.53 usa o cabeçalho HTTP Host para determinar o contexto de um documento fornecido em uma resposta (1) 4xx ou (2) 5xx CONNECT de um servidor proxy, que permite ao usuário - in-the-middle atacantes para executar script web arbitrário, modificando essa resposta CONNECT, também conhecido como um ataque "adulteração SSL".
CVE-2009-1828	O Mozilla Firefox 3.0.10 permite que atacantes remotos causem uma negação de serviço (loop infinito, interrupção de aplicativo e consumo de memória) por meio de um elemento KEYGEN em conjunto com (1) um elemento META especificando atualização automática de página ou (2) um evento onLoad JavaScript manipulador para um elemento BODY. OBSERVAÇÃO: foi informado posteriormente que versões anteriores também são afetadas.
CVE-2009-1690	A vulnerabilidade de usar o after-free no WebKit, como usada no Apple Safari antes do 4.0, iPhone OS 1.0 a 2.2.1, iPhone OS para o iPod touch 1.1 até 2.2.1, Google Chrome 1.0.154.53 e possivelmente outros produtos, permite ataques remotos executar código arbitrário ou causar uma negação de serviço (corrupção de memória e falha de aplicativo) definindo uma propriedade não especificada de uma marca HTML que faz com que elementos filho sejam liberados e acessados posteriormente quando ocorre um erro de HTML relacionado à "recursão em determinado evento DOM manipuladores."
CVE-2009-1598	O Google Chrome executa chamadas DOM em resposta a um javascript: URI no atributo de destino de um elemento de envio em um formulário contido em um arquivo PDF embutido, o que pode permitir que atacantes remotos contornem restrições de JavaScript do Adobe Acrobat ao acessar o objeto de documento, conforme demonstrado por um site que permite uploads de PDF por usuários não confiáveis e, portanto, tem um documento compartilhado.domínio entre o site e este javascript: URI. NOTA: o pesquisador informa que a posição da Adobe é "um arquivo PDF é um conteúdo ativo".
CVE-2009-1514	O Google Chrome 1.0.154.53 permite que atacantes remotos causem uma negação de serviço (desreferenciamento de ponteiro NULL e falha de aplicativo) por meio de uma instrução throw com um valor de exceção longo.
CVE-2009-1442	Vários overflows inteiros no Skia, conforme usados no Google Chrome 1.x antes de 1.0.154.64 e 2.x, e possivelmente no Android, podem permitir que atacantes remotos executem código arbitrário no processo de renderização por meio de uma imagem criada (1) ou (2) tela de pintura.
CVE-2009-1441	O estouro de buffer baseado em heap na função ParamTraits <SkBitmap> :: Read no Google Chrome antes de 1.0.154.64 permite que invasores aproveitem o acesso do renderizador para causar uma negação de serviço (falha do aplicativo) ou

Nome	Descrição
CVE-2009-1414	possivelmente executar código arbitrário por meio de vetores relacionados a um bitmap grande que chega ao canal IPC.
CVE-2009-1413	O Google Chrome 2.0.x permite que modificações no objeto global persistam em uma transição de página, o que facilita para os invasores realizarem ataques de XSS universal por meio de vetores não especificados.
CVE-2009-1413	O Google Chrome 1.0.x não cancela tempos limite em uma transição de página, o que facilita para os invasores realizarem ataques XSS universais chamando setTimeout para acionar a execução futura do código JavaScript e, em seguida, modificando document.location para organizar a execução do JavaScript no contexto de um site arbitrário. OBSERVAÇÃO: isso pode ser aproveitado para um ataque remoto ao explorar uma vulnerabilidade de injeção de argumento chromehtml:.
CVE-2009-1412	A vulnerabilidade de injeção de argumento no manipulador de protocolo chromehtml: no Google Chrome anterior à 1.0.154.59, quando invocada pelo Internet Explorer, permite que atacantes remotos determinem a existência de arquivos e abram guias para URLs que não atendem à restrição IsWebSafeScheme por meio de uma página da Web que define document.location como um chromehtml: value, conforme demonstrado pelo uso de um (1) javascript: ou (2) data: URL. OBSERVAÇÃO: isso pode ser aproveitado para o Universal XSS, explorando determinado comportamento envolvendo persistência nas transições de página.
CVE-2009-0945	Erro de índice de matriz no método insertItemBefore no WebKit, conforme usado no Apple Safari antes de 3.2.3 e 4 Beta Público, iPhone OS 1.0 a 2.2.1, iPhone OS para iPod touch 1.1 a 2.2.1, Google Chrome Estável antes de 1.0.154.65 e, possivelmente, outros produtos permitem que atacantes remotos executem código arbitrário por meio de um documento com uma estrutura de dados SVGPathList contendo um índice negativo no (1) SVGTransformList, (2) SVGStringList, (3) SVGNumberList, (4) SVGPathSegList, (5) SVGPointList ou (6) objeto SVGListList SVGList, que aciona a corrupção de memória.
CVE-2009-0411	O Google Chrome anterior a 1.0.154.46 não restringe adequadamente o acesso de páginas da Web aos cabeçalhos de resposta HTTP (1) Set-Cookie e (2) Set-Cookie2, que permitem que atacantes remotos obtenham informações confidenciais de cookies por meio de chamadas XMLHttpRequest e outros scripts da web .
CVE-2009-0374	** DISPUTADO ** O Google Chrome 1.0.154.43 permite que atacantes remotos induzam o usuário a visitar um URL arbitrário por meio de uma ação de clique que move um elemento criado para a posição atual do mouse, relacionada a uma vulnerabilidade de "Clickjacking". OBSERVAÇÃO: um terceiro contesta a relevância desse problema, afirmando que "todo navegador com recursos suficientes é provavelmente continuará suscetível ao comportamento conhecido como clickjacking" e acrescentando que

Nome	Descrição
	o código de exploração "não é uma demonstração válida do problema".
CVE-2009-0276	A vulnerabilidade de vários domínios no mecanismo JavaScript V8 do Google Chrome anterior a 1.0.154.46 permite que atacantes remotos contornem a Política de mesma origem por meio de um script criado que acesse outro frame e leia sua URL completa e possivelmente outras informações confidenciais ou modifique o URL desse quadro, Armação.
CVE-2008-7294	O Google Chrome anterior à versão 4.0.211.0 não pode restringir adequadamente as modificações nos cookies estabelecidos em sessões HTTPS, o que permite que invasores intermediários substituam ou excluam cookies arbitrários por meio de um cabeçalho Set-Cookie em uma resposta HTTP, relacionada à falta de HTTP O Strict Transport Security (HSTS) inclui o recurso SubDomains, também conhecido como um problema de "cookie forcing".
CVE-2008-7246	O Google Chrome 0.2.149.29 e anterior permite que invasores remotos causem uma negação de serviço (navegador inutilizável) chamando a função window.print em um loop, também conhecido como "impressão de ataque DoS", possivelmente um problema relacionado ao CVE-2009-0821.
CVE-2008-7245	O Opera 9.52 e anteriores permitem que atacantes remotos causem uma negação de serviço (navegador inutilizável) chamando a função window.print em um loop, também conhecido como "impressão de ataque DoS", possivelmente um problema relacionado ao CVE-2009-0821.
CVE-2008-7244	O Mozilla Firefox 3.0.1 e anterior permite que atacantes remotos causem uma negação de serviço (travamento do navegador) chamando a função window.print em um loop, também conhecido como "impressão de ataque DoS", possivelmente um problema relacionado ao CVE-2009-0821.
CVE-2008-7061	O gerenciador de dica de ferramenta (chrome / views / tooltip_manager.cc) no Google Chrome 0.2.149.29 Build 1798 e possivelmente outras versões anteriores a 0.2.149.30 permitem que atacantes remotos causem uma negação de serviço (consumo de CPU ou falha) por meio de uma tag com um título longo atributo, que não é tratado corretamente ao exibir uma dica de ferramenta, uma vulnerabilidade diferente da CVE-2008-6994. Observação: há informações inconsistentes sobre os ambientes em que esse problema existe.
CVE-2008-6998	O estouro de buffer baseado em pilha em chrome / common / gfx / url_elider.cc no Google Chrome 0.2.149.27 e em outras versões anteriores a 0.2.149.29 pode permitir que atacantes remotos assistidos por usuário executem código arbitrário por meio de um link de destino (atributo href) com um grande número de elementos de caminho, que aciona o estouro quando a barra de status é atualizada depois que o usuário passa o mouse sobre o link.

Nome	Descrição
CVE-2008-6997	O Google Chrome 0.2.149.27 permite que invasores remotos assistidos por usuário causem uma negação de serviço (pane no navegador) por meio de uma tag IMG com um atributo src longo, que aciona o travamento quando a vítima realiza uma ação "Inspecionar elemento".
CVE-2008-6996	O Google Chrome BETA (0.2.149.27) não avisa o usuário antes de salvar um arquivo executável, o que facilita para atacantes remotos ou malwares causar uma negação de serviço (consumo de disco) ou explorar outras vulnerabilidades por meio de uma URL que faz referência a um arquivo executável , possivelmente relacionado à configuração "perguntar onde salvar cada arquivo antes de fazer o download".
CVE-2008-6995	O underflow inteiro em net / base / escape.cc no chrome.dll no Google Chrome 0.2.149.27 permite que atacantes remotos causem uma negação de serviço (falha do navegador) por meio de um URI com um manipulador inválido seguido por um caractere "%" (por cento) , que aciona um buffer over-read, conforme demonstrado usando um "about:%" URI.
CVE-2008-6994	O estouro de buffer baseado em pilha no recurso SaveAs (função SaveFileAsWithFilter) em win_util.cc no Google Chrome 0.2.149.27 permite que atacantes remotos assistidos por usuário executem código arbitrário por meio de uma página da Web com um elemento TITLE longo, que aciona o estouro quando o usuário salva a página e um nome de arquivo longo é gerado. NOTA: talvez seja possível explorar esse problema por meio de uma resposta HTTP que inclua um nome de arquivo longo em um cabeçalho Content-Disposition.
CVE-2008-5915	Uma função não especificada na implementação do JavaScript no Google Chrome cria e expõe uma "pegada temporária" quando há um login atual em um site, o que facilita para que invasores remotos induzam o usuário a agir em uma mensagem pop-up falsificada, também conhecido como "ataque de phishing em sessão". NOTA: a partir de 2009 0116, a única divulgação é um pré-aviso vago, sem informações acionáveis. No entanto, como é de um pesquisador conhecido, está sendo atribuído um identificador CVE para fins de rastreamento.
CVE-2008-5750	A vulnerabilidade de injeção de argumento no Microsoft Internet Explorer 8 beta 2 no Windows XP SP3 permite que atacantes remotos executem comandos arbitrários por meio da opção --renderer-path em um chromehtml: URI.
CVE-2008-5749	** DISPUTA ** A vulnerabilidade de injeção de argumento no Google Chrome 1.0.154.36 no Windows XP SP3 permite que atacantes remotos executem comandos arbitrários por meio da opção --renderer-path em um chromehtml: URI. OBSERVAÇÃO: um terceiro contesta esse problema, afirmando que o Chrome "solicitará permissão de usuário" e "não poderá iniciar o applet mesmo [se] você tiver concedido a permissão".
CVE-2008-4724	Várias vulnerabilidades de cross-site scripting (XSS) no Google

Nome	Descrição
	Chrome 0.2.149.30 permitem que invasores remotos injetem scripts web ou HTML arbitrários por meio de um ftp: // URL para um documento HTML em um (1) JPG, (2) PDF ou (3) arquivo TXT. NOTA: a procedência desta informação é desconhecida; os detalhes são obtidos exclusivamente de informações de terceiros.
CVE-2008-4340	O Google Chrome 0.2.149.29 e 0.2.149.30 permite que atacantes remotos causem uma negação de serviço (consumo de memória) por meio de um documento HTML contendo um argumento de retorno de carro ("\ r \ n \ r \ n") para a função window.open.
CVE-2007-0048	Plugin do Adobe Acrobat Reader antes de 8.0.0, e possivelmente o plugin distribuído com o Adobe Reader 7.x antes do 7.1.4, 8.x antes do 8.1.7 e 9.x antes do 9.2, quando usado com o Internet Explorer, Google Chrome ou O Opera, permite que atacantes remotos causem uma negação de serviço (consumo de memória) por meio de uma longa sequência de caracteres # (hash) anexados a uma URL de PDF, relacionada a um "problema de script entre sites".
CVE-2007-0045	Várias vulnerabilidades de cross-site scripting (XSS) no Plug-in do Adobe Acrobat Reader antes de 8.0.0 e possivelmente o plugin distribuído com o Adobe Reader 7.x antes do 7.1.4, 8.x antes do 8.1.7 e 9.x antes do 9.2, para o Mozilla Firefox, o Microsoft Internet Explorer 6 SP1, o Google Chrome, o Opera 8.5.4 build 770 e o Opera 9.10.8679 no Windows permitem que atacantes remotos injetem JavaScript arbitrário e conduzam outros ataques por meio de uma URL .pdf com um javascript: ou res: URI com (1) FDF, (2) XML e (3) parâmetros XFDF AJAX, ou (4) um identificador de âncora arbitrariamente denominado name = URI, também conhecido como "Universal XSS (UXSS)".

Experiência 1.2 - *Common Vulnerabilities and Exposures (CVE)*

A *Common Vulnerabilities and Exposures (CVE)* identifica vulnerabilidades (de projeto e codificação) existentes em software comercial ou aberto, com identificador com formato CVE-AAAA-NNNN, sendo AAAA o ano em que a vulnerabilidade foi catalogada e NNN o seu número.

Aceda a <https://cve.mitre.org/> e verifique:

- o detalhe da vulnerabilidade mais recente;

CVE-2018-10121

plugins / box / pages / pages.admin.php em Monstra O CMS 3.0.4 tem uma vulnerabilidade XSS armazenada quando um invasor tem acesso à função de editor e

entra na carga na seção de título de um admin / index.php? id = pages & action = edit_page & name = error404 (também conhecido como Editar página 404).

- as vulnerabilidades identificadas no Google Chrome

Nome	Descrição
CVE-2012-2870	A libxslt 1.1.26 e anterior, como usada no Google Chrome antes de 21.0.1180.89, não gerencia adequadamente a memória, o que pode permitir que atacantes remotos causem uma negação de serviço (falha do aplicativo) por meio de uma expressão XSLT criada que não seja adequadamente identificada durante o XPath navegação, relacionada a (1) a função xsltCompileLocationPathPattern em libxslt / pattern.c e (2) a função xsltGenerateIdFunction em libxslt / functions.c.
CVE-2012-1846	O Google Chrome 17.0.963.66 e anteriores permitem que atacantes remotos contornem o mecanismo de proteção de sandbox, aproveitando o acesso a um processo de área restrita, conforme demonstrado pela VUPEN durante uma competição Pwn2Own na CanSecWest 2012. OBSERVAÇÃO: o principal produto afetado pode ser esclarecido posteriormente; Não foi identificado pelo pesquisador, que teria declarado que "realmente não importa se é um código de terceiros".
CVE-2012-1845	A vulnerabilidade "usar-depois-livre" no Google Chrome 17.0.963.66 e anterior permite que atacantes remotos contornem os mecanismos de proteção DEP e ASLR e executem código arbitrário, por meio de vetores não especificados, conforme demonstrado pela VUPEN durante uma competição Pwn2Own no CanSecWest 2012. OBSERVAÇÃO: o produto primário afetado pode ser esclarecido posteriormente; Não foi identificado pelo pesquisador, que teria declarado que "realmente não importa se é um código de terceiros".

Há **47** entradas CVE que correspondem à sua pesquisa em relação as vulnerabilidades do Facebook

Nome	Descrição
------	-----------

Nome	Descrição
CVE-2018-6858	O Cross Site Scripting (XSS) existe no Script PHP do Facebook Scripts Mall.
CVE-2018-6367	O SQL Injection existe no Clone 2.9.9 do Vastal I-Tech Buddy Zone através do parâmetro /chat_im/chat_window.php request_id ou do parâmetro de categoria /search_events.php.
CVE-2018-5978	Injeção de SQL existe no Estilo do Facebook Php Ajax Chat Zechat 1.5 através do campo Usuário do login.php.
CVE-2018-5214	O plugin "Add Link to Facebook" através do 2.3 para WordPress tem o XSS através do parâmetro al2fb_facebook_id para o wp-admin / profile.php.
CVE-2017-8769	** DISPUTA ** Facebook WhatsApp Messenger antes de 2.16.323 para Android usa o cartão SD para armazenamento de arquivos em texto puro (Áudio, Documentos, Imagens, Vídeo e Notas de voz) associados a um bate-papo, mesmo depois que o bate-papo é excluído. Pode haver usuários que esperam que a exclusão de arquivos ocorra após a exclusão do bate-papo ou que esperem criptografia (consistente com o uso do aplicativo de um banco de dados criptografado para armazenar o texto do bate-papo). OBSERVAÇÃO: o fornecedor indica que ele não "considera esses problemas de segurança" porque um usuário pode legitimamente preservar qualquer arquivo para uso "em outros aplicativos, como a galeria do Google Fotos", independentemente de o bate-papo associado ser excluído.

Experiência 1.3 - **Common Vulnerability Scoring System (CVSS)**

O Common Vulnerability Scoring System (CVSS) disponibiliza um modelo quantitativo para definir as características e impacto das vulnerabilidades, garantindo uma medição precisa e repetível para gerar pontuações de impacto de vulnerabilidade.

Dois usos comuns do CVSS são a priorização das atividades de correção de vulnerabilidades e, o cálculo da gravidade das vulnerabilidades descobertas.

Explore o calculador de vulnerabilidades em <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

As pontuações são calculadas em sequência de tal forma que a Pontuação Básica é usada para calcular a Pontuação Temporal e a Pontuação Temporal é usada para calcular a Pontuação

Métricas de pontuação básica

- **Métricas de exploração**
- Vetor de ataque (AV) *
- Rede (AV: N) Rede Adjacente (AV: A) Local (AV: L) Físico (AV: P)
- Complexidade de ataque (CA) *
- Baixo (AC: L) Alta (AC: H)
- Privilégios requeridos (PR) *
- Nenhum (PR: N) Baixo (PR: L) Alta (PR: H)
- Interação do usuário (UI) *
- Nenhum (UI: N) Obrigatório (UI: R)
- Escopo (S) *
- Inalterado (S: U) Alterado (S: C)
- **Métricas de impacto**
- Impacto de Confidencialidade (C) *
- Nenhum (C: N) Baixo (C: L) Alta (C: H)
- Impacto da Integridade (I) *
- Nenhum (I: N) Baixo (I: L) Alta (I: H)
- Impacto da Disponibilidade (A) *
- Nenhum (A: N) Baixo (A: L) Alta (A: H)

Métricas de pontuação temporal

- Explorabilidade (E)
- Não definido (E: X)Não comprovado que a exploração existe (E: U)Código de prova de conceito (E: P)A exploração funcional existe (E: F)Alta (E: H)
- Nível de correção (RL)
- Não definido (RL: X)Correção oficial (RL: O)Correção temporária (RL: T)Solução alternativa (RL: W)Indisponível (RL: U)
- Comunicar Confiança (RC)
- Não definido (RC: X)

- Desconhecido (RC: U)Razoável (RC: R)Confirmado (RC: C)

Métricas de Pontuação Ambiental

• **Modificadores de base**

- Vetor de ataque (AV)
- Não definido (MAV: X)Rede (MAV: N)Rede Adjacente (MAV: A)Local (MAV: L)Físico (MAV: P)
- Complexidade de ataque (AC)
- Não definido (MAC: X)Baixo (MAC: L)Alta (MAC: H)
- Privilégios Requeridos (PR)
- Não definido (MPR: X)Nenhum (MPR: N)Baixo (MPR: L)Alta (MPR: H)
- Interação do usuário (UI)
- Não definido (MUI: X)Nenhum (MUI: N)Obrigatório (MUI: R)
- Âmbito (s)
- Não Definido (MS: X)Inalterado (MS: U)Alterado (MS: C)

• **Métricas de impacto**

- Impacto de Confidencialidade (C)
- Não definido (MC: X)Nenhum (MC: N)Baixo (MC: L)Alta (MC: H)
- Impacto da Integridade (I)
- Não Definido (MI: X)Nenhum (MI: N)Baixo (MI: L)Alta (MI: H)
- Impacto da Disponibilidade (A)
- Não Definido (MA: X)Nenhum (MA: N)Baixo (MA: L)Alta (MA: H)

• **Modificadores de Subcore de Impacto**

- Requisito de Confidencialidade (CR)
- Não definido (CR: X)Baixo (CR: L)Médio (CR: M)Alta (CR: H)
- Requisito de integridade (IR)
- Não definido (IR: X)Baixo (IR: L)Médio (IR: M)Alta (IR: H)
- Requisito de disponibilidade (AR)
- Não definido (AR: X)Baixo (AR: L)Médio (AR: M)Alta (AR: H)

Experiência 1.4 - National Vulnerability Database (NVD)

A *National Vulnerability Database* (NVD) é o repositório de vulnerabilidades gerido pelo NIST. Baseia-se no CVE, mas inclui a gravidade da vulnerabilidade, de acordo com o CVSS (*Common Vulnerability Scoring System*)

Aceda a <https://nvd.nist.gov/> e verifique:

- qual é a vulnerabilidade mais recente identificada?

CVE-2007-2619

O Symantec pcAnywhere 11.5.xe 12.0.x mantém as credenciais de login não criptografadas para o login mais recente na memória de processo, o que permite que os administradores locais obtenham as credenciais lendo a memória do processo, uma vulnerabilidade diferente da CVE-2006-3785.

Publicado em: 11 de maio de 2007; - das 12: 19h às 04: 00h;

- essa vulnerabilidade é a mesma vulnerabilidade mais recente encontrada na experiência 1.2 (CVE)? Qual poderá ser o motivo?

R: Não é a mesma vulnerabilidade porque, embora um ID CVE possa ter sido atribuído por um CVE ou por um CAN ele não estará disponível no NVD se tiver um status reservado pelo CVE

- as vulnerabilidades identificadas no Google Chrome;

Existem **467** registros correspondentes relacionados com as vulnerabilidades identificadas no Google Chrome mas faremos menção das mais recentes

CVE-2016-5175

Várias vulnerabilidades não especificadas no Google Chrome anteriores a 53.0.2785.113 permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.

Publicado em: 25 de setembro de 2016; 04:59:08 PM -04: 00

CVE-2016-5167

Várias vulnerabilidades não especificadas no Google Chrome anteriores a 53.0.2785.89 no Windows e no OS X e anteriores a 53.0.2785.92 no Linux permitem que invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.

Publicado em: 11 de setembro de 2016; 06:59:24 AM-04: 00

CVE-2016-5146

Várias vulnerabilidades não especificadas no Google Chrome anteriores a 52.0.2743.116 permitem que os invasores causem uma negação de serviço ou possivelmente tenham outro impacto por meio de vetores desconhecidos.

Publicado em 07 de agosto de 2016; 03:59:11 PM -04: 00

- as vulnerabilidades identificadas no Facebook.

Existem **16** registros correspondentes relacionados com as vulnerabilidades identificadas no Facebook mas faremos menção das mais recentes.

CVE-2018-5214

O plugin "Add Link to Facebook" através do 2.3 para WordPress tem o XSS através do parâmetro al2fb_facebook_id para o wp-admin / profile.php.

Publicado em: 04 de janeiro de 2018; 01:29:00 PM -05: 00

CVE-2016-2350

Várias vulnerabilidades de cross-site scripting (XSS) no Acceleration File Transfer Appliance (FTA) antes de FTA_9_12_40 permitir que invasores remotos injetem script web arbitrário ou HTML via entrada não especificada para (1) getimageajax.php, (2) move_partition_frame.html, ou (3) wmlInfo.html.

Publicado em: 07 de maio de 2016; 10:59:03 AM - 04:00

Pergunta P1.1

Em <https://informationisbeautiful.net/visualizations/million-lines-of-code/> encontra (algumas são estimativas) o número de linha de código (*SLOC - Source Lines Of Code*) de alguns pacotes/plataformas de software.

1. Estime o número de bugs do Facebook, software de automóveis, Linux 3.1 e de todos os serviços Internet da Google.
 - Facebook tem aproximadamente 61 bugs
 - software de automóveis tem aproximadamente 100 bugs
 - Linux 3.1 tem aproximadamente 15 bugs
2. Quantos desses bugs são vulnerabilidades?

Os software que são aplicação são mais vulneráveis logo temos os bugs Facebook .

Pergunta P1.2

Considere os três tipos de vulnerabilidades: de projeto, de codificação e operacional. Apresente para cada um deles dois exemplos e discuta a dificuldade de correção.

2 vulnerabilidades de projectos:

CWE-7: Configuração incorreta do J2EE: página de erro personalizada ausente

ID de fraqueza: 7

Status: incompleto

Abstração: Estrutura Variante

: Simples

Filtro de Apresentação:



Descrição

A página de erro padrão de um aplicativo da Web não deve exibir informações confidenciais sobre o sistema de software.

▼ Descrição estendida

Um aplicativo da Web deve definir uma página de erro padrão para erros 4xx (por exemplo, 404), 5xx (por exemplo, 500) e capturar exceções java.lang.Throwable para impedir que invasores extraiam informações da resposta de erro interna do contêiner do aplicativo.

Quando um invasor explora um site procurando vulnerabilidades, a quantidade de informações que o site fornece é crucial para o eventual sucesso ou fracasso de qualquer tentativa de ataque.

▼ Relacionamentos

A tabela abaixo mostra as fraquezas e categorias de alto nível relacionadas a essa fraqueza. Esses relacionamentos são definidos como ChildOf, ParentOf, MemberOf e fornecem informações sobre itens semelhantes que podem existir em níveis mais altos e mais baixos de abstração. Além disso, relacionamentos como PeerOf e CanAlsoBe são definidos para mostrar pontos fracos semelhantes que o usuário pode querer explorar.

- ▶ Relevante para a visão "Research Concepts" (CWE-1000)
- ▶ Relevante para a visão "Conceitos de Desenvolvimento" (CWE-699)

▼ Modos de Introdução

Os diferentes Modos de Introdução fornecem informações sobre como e quando essa fraqueza pode ser introduzida. A fase identifica um ponto no ciclo de vida do software no qual a introdução pode ocorrer, enquanto a nota fornece um cenário típico relacionado à introdução durante a fase determinada.

▼ Plataformas Aplicáveis

As listas abaixo mostram possíveis áreas para as quais a fraqueza dada pode aparecer. Estes podem ser para linguagens específicas nomeadas, sistemas operacionais, arquiteturas, paradigmas, tecnologias ou uma classe de tais plataformas. A plataforma é listada juntamente com a frequência com que a fraqueza determinada aparece para essa instância.

línguas

Java (Prevalência Indeterminada)

▼ Consequências Comuns

A tabela abaixo especifica diferentes consequências individuais associadas à fraqueza. O Escopo identifica a área de segurança do aplicativo que é violada, enquanto o Impacto descreve o impacto técnico negativo que surge quando um adversário consegue explorar essa vulnerabilidade. A Verossimilhança fornece informações sobre a probabilidade de a consequência específica ser vista em relação às outras consequências na lista. Por exemplo, pode haver uma alta probabilidade de que uma fraqueza seja explorada para alcançar um certo impacto, mas uma baixa probabilidade de ser explorada para alcançar um impacto diferente.

Escopo	Impacto	Probabilidade
Confidencialidade	<p>Impacto Técnico: Ler Dados da Aplicação</p> <p>Um rastreamento de pilha pode mostrar ao invasor uma cadeia de consulta SQL malformada, o tipo de banco de dados que está sendo usado e a versão do contêiner do aplicativo. Essas informações permitem que o invasor segmente vulnerabilidades conhecidas nesses componentes.</p>	

▼ Exemplos demonstrativos

Exemplo 1

No snippet abaixo, uma exceção de tempo de execução não verificada lançada de dentro do bloco try pode fazer com que o contêiner exiba sua página de erro padrão (que pode conter um rastreamento de pilha completo, entre outras coisas).

(código ruim)

Idioma de exemplo: Java

```
Public void doPost (solicitação HttpServletRequest, resposta HttpServletResponse) lança  
ServletException, IOException {
```

```
experimentar {
```

```
...
```

```
} catch (ApplicationSpecificException ase) {
```

```
logger.error ("Capturado:" + ase.toString());
```

```
}
```

```
}
```

▼ Mitigações Potenciais

Fase: Implementação

Lidar com exceções apropriadamente no código-fonte.

Fases: Implementação; Configuração do sistema

Sempre defina as páginas de erro apropriadas. A configuração do aplicativo deve especificar uma página de erro padrão para garantir que o aplicativo nunca vaze mensagens de erro para um invasor. A manipulação de códigos de erro HTTP padrão é útil e amigável ao usuário, além de ser uma boa prática de segurança, e uma boa configuração também definirá um manipulador de erros de última chance que detecta qualquer exceção que possa ser lançada pelo aplicativo.

Fase: Implementação

Não tente processar um erro ou tentar mascará-lo.

Fase: Implementação

Verifique se os valores de retorno estão corretos e não forneça informações confidenciais sobre o sistema.

▼ Assocações

Esta tabela Relacionamentos MemberOf mostra Categorias e Exibições CWE adicionais que fazem referência a essa vulnerabilidade como um membro. Esta informação é frequentemente útil para entender onde uma fraqueza se encaixa dentro do contexto de fontes externas de informação.

CWE-6: Configuração incorreta do J2EE: comprimento de ID de sessão insuficiente

ID de fraqueza: 6

Status: incompleto

Abstração: Estrutura Variante

: Simples

Filtro de Apresentação:



▼ Descrição

O aplicativo J2EE está configurado para usar um comprimento de ID de sessão insuficiente.

▼ Descrição estendida

Se um invasor puder adivinhar ou roubar um ID de sessão, poderá assumir a sessão do usuário (chamado de seqüestro de sessão). O número de IDs de sessão possíveis aumenta com o aumento da duração do ID da sessão, dificultando a adivinhação ou o roubo de um ID de sessão.

▼ Relacionamentos

A tabela abaixo mostra as fraquezas e categorias de alto nível relacionadas a essa fraqueza. Esses relacionamentos são definidos como ChildOf, ParentOf, MemberOf e fornecem informações sobre itens semelhantes que podem existir em níveis mais altos e

mais baixos de abstração. Além disso, relacionamentos como PeerOf e CanAlsoBe são definidos para mostrar pontos fracos semelhantes que o usuário pode querer explorar.

- ▶ Relevante para a visão "Research Concepts" (CWE-1000)
 - ▶ Relevante para a visão "Conceitos Arquitetônicos" (CWE-1008)
 - ▶ Relevante para a visão "Conceitos de Desenvolvimento" (CWE-699)
- ▼ Modos de Introdução

Os diferentes Modos de Introdução fornecem informações sobre como e quando essa fraqueza pode ser introduzida. A fase identifica um ponto no ciclo de vida do software no qual a introdução pode ocorrer, enquanto a nota fornece um cenário típico relacionado à introdução durante a fase determinada.

Estágio	Nota
Arquitetura e Design	COMISSÃO: Esta fraqueza refere-se a um projeto incorreto relacionado a uma tática de segurança arquitetônica.
Implementação	

▼ Plataformas Aplicáveis

As listas abaixo mostram possíveis áreas para as quais a fraqueza dada pode aparecer. Estes podem ser para linguagens específicas nomeadas, sistemas operacionais, arquiteturas, paradigmas, tecnologias ou uma classe de tais plataformas. A plataforma é listada juntamente com a frequência com que a fraqueza determinada aparece para essa instância.

Línguas

Java (Prevalência Indeterminada)

▼ Consequências Comuns

A tabela abaixo especifica diferentes consequências individuais associadas à fraqueza. O Escopo identifica a área de segurança do aplicativo que é violada, enquanto o Impacto descreve o impacto técnico negativo que surge quando um adversário consegue explorar essa vulnerabilidade. A Verossimilhança fornece informações sobre a probabilidade de a consequência específica ser vista em relação às outras consequências na lista. Por exemplo, pode haver uma alta probabilidade de que uma fraqueza seja explorada para alcançar um certo impacto, mas uma baixa probabilidade de ser explorada para alcançar um impacto diferente.

Escopo	Impacto	Probabilidade
Controle de acesso	Impacto Técnico: Ganhe Privilégios ou Assuma a Identidade Se um invasor puder adivinhar o identificador de sessão de um usuário autenticado, ele poderá assumir a sessão do usuário.	

▼ Exemplos demonstrativos

Exemplo 1

O seguinte código de exemplo XML é um descritor de implantação para um aplicativo da Web Java implementado em um Sun Java Application Server. Esse descritor de implantação inclui uma propriedade de configuração de sessão para configurar o comprimento do ID da sessão.

(código ruim)

Linguagem de Exemplo: XML

```
<sun-web-app>
...
<session-config>
<session-properties>
<nome da propriedade = "idLengthBytes" value = "8">
<description> O número de bytes no ID de sessão deste módulo da web. </description>
</property>
</ session-properties>
</ session-config>
...
</ sun-web-app>
```

Este descritor de implementação definiu o comprimento do ID da sessão para este aplicativo da Web Java para 8 bytes (ou 64 bits). O comprimento do ID da sessão para aplicativos da Web Java deve ser definido como 16 bytes (128 bits) para evitar que invasores adivinhem e / ou roubem uma ID de sessão e assumam a sessão de um usuário.

Nota para a maioria dos servidores de aplicativos, incluindo o Sun Java Application Server, o tamanho da ID da sessão é, por padrão, definido como 128 bits e não deve ser alterado. E para muitos servidores de aplicativos, o comprimento do ID da sessão não pode ser alterado a partir dessa configuração padrão. Verifique a documentação do servidor de aplicativos para obter as configurações padrão e a opção de comprimento do ID da sessão para assegurar que o comprimento do ID da sessão esteja configurado para 128 bits.

▼ Mitigações Potenciais

Fase: Implementação

Os identificadores de sessão devem ter pelo menos 128 bits para evitar adivinhação de sessão de força bruta. Um identificador de sessão mais curto deixa o aplicativo aberto para ataques de adivinhação de sessão de força bruta.

Fase: Implementação

Um limite inferior no número de identificadores de sessão válidos que estão disponíveis para serem adivinhados é o número de usuários ativos em um site a qualquer

momento. No entanto, qualquer usuário que abandonar suas sessões sem efetuar logout aumentará esse número. (Esse é um dos muitos bons motivos para ter um tempo limite curto de sessão inativa.) Com um identificador de sessão de 64 bits, considere 32 bits de entropia. Para um site grande, assuma que o invasor pode tentar 1.000 estimativas por segundo e que existem 10.000 identificadores de sessão válidos a qualquer momento. Dadas essas suposições, o tempo esperado para um invasor adivinhar com sucesso um identificador de sessão válido é menor que 4 minutos. Agora, assuma um identificador de sessão de 128 bits que forneça 64 bits de entropia. Com um site muito grande, um invasor pode tentar 10.000 palpites por segundo com 100, 000 identificadores de sessão válidos disponíveis para serem adivinhados. Dadas essas suposições, o tempo esperado para um invasor adivinhar com sucesso um identificador de sessão válido é maior que 292 anos.

▼ Assocações

Esta tabela Relacionamentos MemberOf mostra Categorias e Exibições CWE adicionais que fazem referência a essa vulnerabilidade como um membro. Esta informação é frequentemente útil para entender onde uma fraqueza se encaixa dentro do contexto de fontes externas de informação.

2 vulnerabilidades de codificação:

CWE-5: Configuração incorreta do J2EE: transmissão de dados sem criptografia

ID de fraqueza: 5

Status: rascunho

Abstração: Estrutura Variante

: Simples

Filtro de Apresentação:

▼ Descrição

As informações enviadas por uma rede podem ficar comprometidas durante o trânsito. Um invasor pode ler ou modificar o conteúdo se os dados forem enviados em texto sem formatação ou forem criptografados fracamente.

▼ Relacionamentos

A tabela abaixo mostra as fraquezas e categorias de alto nível relacionadas a essa fraqueza. Esses relacionamentos são definidos como ChildOf, ParentOf, MemberOf e fornecem informações sobre itens semelhantes que podem existir em níveis mais altos e mais baixos de abstração. Além disso, relacionamentos como PeerOf e CanAlsoBe são definidos para mostrar pontos fracos semelhantes que o usuário pode querer explorar.

- ▶ Relevante para a visão "Research Concepts" (CWE-1000)
- ▶ Relevante para a visão "Conceitos de Desenvolvimento" (CWE-699)

▼ Modos de Introdução

Os diferentes Modos de Introdução fornecem informações sobre como e quando essa fraqueza pode ser introduzida. A fase identifica um ponto no ciclo de vida do software no qual a introdução pode ocorrer, enquanto a nota fornece um cenário típico relacionado à introdução durante a fase determinada.

▼ Plataformas Aplicáveis

As listas abaixo mostram possíveis áreas para as quais a fraqueza dada pode aparecer. Estes podem ser para linguagens específicas nomeadas, sistemas operacionais, arquiteturas, paradigmas, tecnologias ou uma classe de tais plataformas. A plataforma é listada juntamente com a frequência com que a fraqueza determinada aparece para essa instância.

Línguas

Java (Prevalência Indeterminada)

▼ Consequências Comuns

A tabela abaixo especifica diferentes consequências individuais associadas à fraqueza. O Escopo identifica a área de segurança do aplicativo que é violada, enquanto o Impacto descreve o impacto técnico negativo que surge quando um adversário consegue explorar essa vulnerabilidade. A Verossimilhança fornece informações sobre a probabilidade de a consequência específica ser vista em relação às outras consequências na lista. Por exemplo, pode haver uma alta probabilidade de que uma fraqueza seja explorada para alcançar um certo impacto, mas uma baixa probabilidade de ser explorada para alcançar um impacto diferente.

Escopo	Impacto	Probabilidade
Confidencialidade	Impacto Técnico: Ler Dados da Aplicação	
Integridade	Impacto Técnico: Modificar Dados da Aplicação	

▼ Mitigações Potenciais

Fase: configuração do sistema

A configuração do aplicativo deve garantir que o SSL ou um mecanismo de criptografia de força equivalente e reputação verificada seja usado para todas as páginas controladas por acesso.

▼ Associações

Esta tabela Relacionamentos MemberOf mostra Categorias e Exibições CWE adicionais que fazem referência a essa vulnerabilidade como um membro. Esta informação é frequentemente útil para entender onde uma fraqueza se encaixa dentro do contexto de fontes externas de informação.

As 2 vulnerabilidades de configuração são:

CWE-6: Configuração incorreta do J2EE: comprimento de ID de sessão insuficiente

ID de fraqueza: 6

Status: incompleto

Abstração: Estrutura Variante

: Simples

Filtro de Apresentação:



▼ Descrição

O aplicativo J2EE está configurado para usar um comprimento de ID de sessão insuficiente.

▼ Descrição estendida

Se um invasor puder adivinhar ou roubar um ID de sessão, poderá assumir a sessão do usuário (chamado de seqüestro de sessão). O número de IDs de sessão possíveis aumenta com o aumento da duração do ID da sessão, dificultando a adivinhação ou o roubo de um ID de sessão.

▼ Relacionamentos

A tabela abaixo mostra as fraquezas e categorias de alto nível relacionadas a essa fraqueza. Esses relacionamentos são definidos como ChildOf, ParentOf, MemberOf e fornecem informações sobre itens semelhantes que podem existir em níveis mais altos e mais baixos de abstração. Além disso, relacionamentos como PeerOf e CanAlsoBe são definidos para mostrar pontos fracos semelhantes que o usuário pode querer explorar.

- ▶ Relevante para a visão "Research Concepts" (CWE-1000)
- ▶ Relevante para a visão "Conceitos Arquitetônicos" (CWE-1008)
- ▶ Relevante para a visão "Conceitos de Desenvolvimento" (CWE-699)

▼ Modos de Introdução

Os diferentes Modos de Introdução fornecem informações sobre como e quando essa fraqueza pode ser introduzida. A fase identifica um ponto no ciclo de vida do software no qual a introdução pode ocorrer, enquanto a nota fornece um cenário típico relacionado à introdução durante a fase determinada.

Estágio	Nota
Arquitetura e Design	COMISSÃO: Esta fraqueza refere-se a um projeto incorreto relacionado a uma tática de segurança arquitetônica.
Implementação	

▼ Plataformas Aplicáveis

As listas abaixo mostram possíveis áreas para as quais a fraqueza dada pode aparecer. Estes podem ser para linguagens específicas nomeadas, sistemas operacionais, arquiteturas, paradigmas, tecnologias ou uma classe de tais plataformas. A plataforma é listada juntamente com a frequência com que a fraqueza determinada aparece para essa instância.

Línguas

Java (Prevalência Indeterminada)

▼ Consequências Comuns

A tabela abaixo especifica diferentes consequências individuais associadas à fraqueza. O Escopo identifica a área de segurança do aplicativo que é violada, enquanto o Impacto descreve o impacto técnico negativo que surge quando um adversário consegue explorar essa vulnerabilidade. A Verossimilhança fornece informações sobre a probabilidade de a consequência específica ser vista em relação às outras consequências na lista. Por exemplo, pode haver uma alta probabilidade de que uma fraqueza seja explorada para alcançar um certo impacto, mas uma baixa probabilidade de ser explorada para alcançar um impacto diferente.

Escopo	Impacto	Probabilidade
Controle de acesso	Impacto Técnico: Ganhe Privilégios ou Assuma a Identidade Se um invasor puder adivinhar o identificador de sessão de um usuário autenticado, ele poderá assumir a sessão do usuário.	

▼ Exemplos demonstrativos

Exemplo 1

O seguinte código de exemplo XML é um descritor de implantação para um aplicativo da Web Java implementado em um Sun Java Application Server. Esse descritor de implantação inclui uma propriedade de configuração de sessão para configurar o comprimento do ID da sessão.

(código ruim)

Linguagem de Exemplo: XML

```
<sun-web-app>  
...  
<session-config>  
<session-properties>  
<nome da propriedade = "idLengthBytes" value = "8">  
<description> O número de bytes no ID de sessão deste módulo da web. </ description>  
</ property>  
</ session-properties>  
</ session-config>  
...  
</ sun-web-app>
```

Este descritor de implementação definiu o comprimento do ID da sessão para este aplicativo da Web Java para 8 bytes (ou 64 bits). O comprimento do ID da sessão para aplicativos da Web Java deve ser definido como 16 bytes (128 bits) para evitar que

invasores adivinhem e / ou roubem uma ID de sessão e assumam a sessão de um usuário.

Nota para a maioria dos servidores de aplicativos, incluindo o Sun Java Application Server, o tamanho da ID da sessão é, por padrão, definido como 128 bits e não deve ser alterado. E para muitos servidores de aplicativos, o comprimento do ID da sessão não pode ser alterado a partir dessa configuração padrão. Verifique a documentação do servidor de aplicativos para obter as configurações padrão e a opção de comprimento do ID da sessão para assegurar que o comprimento do ID da sessão esteja configurado para 128 bits.

▼ Mitigações Potenciais

Fase: Implementação

Os identificadores de sessão devem ter pelo menos 128 bits para evitar adivinhação de sessão de força bruta. Um identificador de sessão mais curto deixa o aplicativo aberto para ataques de adivinhação de sessão de força bruta.

Fase: Implementação

Um limite inferior no número de identificadores de sessão válidos que estão disponíveis para serem adivinhados é o número de usuários ativos em um site a qualquer momento. No entanto, qualquer usuário que abandonar suas sessões sem efetuar logout aumentará esse número. (Esse é um dos muitos bons motivos para ter um tempo limite curto de sessão inativa.) Com um identificador de sessão de 64 bits, considere 32 bits de entropia. Para um site grande, assuma que o invasor pode tentar 1.000 estimativas por segundo e que existem 10.000 identificadores de sessão válidos a qualquer momento. Dadas essas suposições, o tempo esperado para um invasor adivinhar com sucesso um identificador de sessão válido é menor que 4 minutos. Agora, assuma um identificador de sessão de 128 bits que forneça 64 bits de entropia. Com um site muito grande, um invasor pode tentar 10.000 palpites por segundo com 100, 000 identificadores de sessão válidos disponíveis para serem adivinhados. Dadas essas suposições, o tempo esperado para um invasor adivinhar com sucesso um identificador de sessão válido é maior que 292 anos.

▼ Associações

Esta tabela Relacionamentos MemberOf mostra Categorias e Exibições CWE adicionais que fazem referência a essa vulnerabilidade como um membro. Esta informação é frequentemente útil para entender onde uma fraqueza se encaixa dentro do contexto de fontes externas de informação.

Pergunta P1.3

O que é que distingue uma vulnerabilidade diz-zero de outra vulnerabilidade de codificação que não seja de dia-zero?

As diferenças entre essas vulnerabilidades são:

Uma vulnerabilidade de codificação diz dia-zero, quando não existem correções para minimizar o aproveitamento da *vulnerabilidade*. Enquanto as que não são dia-zero, quando existem correções ou já foram descobertas formas de correção para minimizar o aproveitamento da mesma.

Experiência 1.8

```
user@CSI:~/Aulas$ vim teste.c
user@CSI:~/Aulas$ gcc teste.c
user@CSI:~/Aulas$ ls
a.out Aula2 Aula3 teste.c
user@CSI:~/Aulas$ dir
a.out Aula2 Aula3 teste.c
user@CSI:~/Aulas$ ls -la
total 32
drwxr-xr-x 4 user user 4096 Apr 9 16:41 .
drwxr-xr-x 20 user user 4096 Apr 9 16:40 ..
-rwxr-xr-x 1 user user 8680 Apr 9 16:41 a.out
drwxr-xr-x 5 user user 4096 Feb 10 18:08 Aula2
drwxr-xr-x 2 user user 4096 Feb 19 17:37 Aula3
-rw-r--r-- 1 user user 61 Apr 9 16:40 teste.c
user@CSI:~/Aulas$ ./a.out
Ola Mundouser@CSI:~/Aulas$ vim teste.c
user@CSI:~/Aulas$ gcc teste.c
user@CSI:~/Aulas$ ./a.out
Ola Mundo
user@CSI:~/Aulas$ gcc -S teste.c
user@CSI:~/Aulas$ ls -la
total 36
drwxr-xr-x 4 user user 4096 Apr 9 16:41 .
drwxr-xr-x 20 user user 4096 Apr 9 16:41 ..
-rwxr-xr-x 1 user user 8680 Apr 9 16:41 a.out
drwxr-xr-x 5 user user 4096 Feb 10 18:08 Aula2
drwxr-xr-x 2 user user 4096 Feb 19 17:37 Aula3
-rw-r--r-- 1 user user 63 Apr 9 16:41 teste.c
-rw-r--r-- 1 user user 445 Apr 9 16:41 teste.s
user@CSI:~/Aulas$ more teste.s
.file "teste.c"
.section .rodata
.LC0:
.string "Ola Mundo"
.text
.globl main
.type main, @function
main:
```

```
.LFB0:  
.cfi_startproc  
pushq %rbp  
.cfi_def_cfa_offset 16  
.cfi_offset 6, -16  
movq %rsp, %rbp  
.cfi_def_cfa_register 6  
leaq .LC0(%rip), %rdi  
call puts@PLT  
nop  
popq %rbp  
.cfi_def_cfa 7, 8  
ret  
.cfi_endproc  
.LFE0:  
.size main, .-main  
.ident "GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516"  
.section .note.GNU-stack,"",@progbits  
user@CSI:~/Aulas$  
user@CSI:~/Aulas$  
user@CSI:~/Aulas$  
user@CSI:~/Aulas$ more teste.s  
.file "teste.c"  
.section .rodata  
.LC0:  
.string "Ola Mundo"  
.text  
.globl main  
.type main, @function  
main:  
.LFB0:  
.cfi_startproc  
pushq %rbp  
.cfi_def_cfa_offset 16  
.cfi_offset 6, -16  
movq %rsp, %rbp  
.cfi_def_cfa_register 6  
leaq .LC0(%rip), %rdi  
call puts@PLT  
nop  
popq %rbp  
.cfi_def_cfa 7, 8  
ret  
.cfi_endproc  
.LFE0:  
.size main, .-main  
.ident "GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516"
```

```
.section .note.GNU-stack,"",@progbits  
user@CSI:~/Aulas$
```