

O que há de novo na 9.4.2: Funções de firewall XML

A introdução da versão 9.4.2 do BIG-IP® Application Security Manager (ASM) marca um grande avanço. O BIG-IP ASM agora oferece mais funções, que são mais simples de usar que nas versões anteriores, permitindo uma especificação e inspeção de políticas mais granular, ajudando a manter sua posição na vanguarda dos firewalls de aplicativos web (WAFs).

Na verdade, o BIG-IP ASM versão 9.4.2 é mais do que apenas um WAF. Essa versão do BIG-IP ASM avança em direção ao conceito de segurança de distribuição de aplicativos, permitindo que todos os aplicativos de segundo plano — e não somente os aplicativos web tradicionais, como a maioria dos WAFs atuais — se beneficiem de sua proteção. Assim como os outros produtos da linha BIG-IP, o ASM é parte de uma estratégia ponto-a-ponto que integra a segurança em uma estrutura de distribuição de aplicativos de alto desempenho. A segurança relativa não ao modo como a comunicação com o cliente acontece, mas relativa aos dados que são enviados ao cliente.

A segurança na distribuição de aplicativos oferecida pelo BIG-IP ASM enfoca os próprios dados, independentemente do aplicativo que os distribui. Graças ao poder da TMOS, do Real Time Policy Builder e, como explicado abaixo, das novas funções de Firewall XML, o BIG-IP ASM vai além dos WAFs tradicionais e cria uma visão holística da segurança de aplicativos¹.

Mais diretamente, se o tráfego está nas camadas de 4 a 7, é tráfego de aplicativos, e o BIG-IP ASM pode fazer algo para protegê-lo.

O que faz que essa notação menor ("ponto") pareça tão importante?

Embora muitas das funções representem avanços técnicos ou de uso, esta versão significa uma mudança fundamental no modo como o BIG-IP ASM interage com a rede, usuários e aplicativos. O BIG-IP ASM expande sua capacidade para o nível dos firewalls de aplicativos. Em vez de ser limitado pelas noções do que constitui um aplicativo da web, o BIG-IP ASM examina o tráfego dos aplicativos em busca de problemas de segurança, independentemente do método de distribuição.

Todas as ricas funções que fazem parte dos sites Web 2.0 feitos com as tecnologias AJAX (JavaScript Assíncrono e XML), Ruby no RAILS e JSON (Notação de Objetos JavaScript) agora estão sob a proteção da segurança de distribuição de aplicativos. Os aplicativos distribuídos pela web não são somente os aplicativos que usam as estruturas de trabalho Web 2.0; outros exemplos são o Sales Force Automation (SFA), Enterprise Resource Planning (ERP) e Voz sobre IP (VoIP). Em função de sua visibilidade, complexidade e dos custos de implementação desses tipos de aplicativos, as quebras de segurança de dados podem ser um enorme risco financeiro para as companhias que vêm de um aplicativo web "padrão".

Com essa versão, o foco não é mais em modelos de segurança positivos ou negativos. Esses modos sugerem que as brechas de segurança podem ser caracterizadas por padrões simples e estáticos, que podem ser identificados e bloqueados. O foco do BIG-IP ASM é na lógica nas ações de negócios dos aplicativos, porque há maior risco no abuso da funcionalidade inerente a um aplicativo do que numa quebra direta. Pense nos sites de compras on-line; a quebra

de um site de compras não causa tantos danos nem é tão lucrativa quanto a compra disfarçada dos itens mais populares por centavos.

Ao considerar os aspectos mais amplos da segurança de aplicativos, o BIG-IP ASM muda o modo como os protege. Fundamentalmente, é isso que torna essa versão tão importante.

Proteção de aplicativos no BIG-IP ASM

Como parte do empenho na proteção de dados não depende da distribuição, as capacidades do BIG-IP ASM agora ajudam a proteger contra ataques comuns como a evasão e injeção de comandos SQL, adulteração de parâmetros e ataques de intermediários (man in the middle). Um dos maiores aumentos na capacidade vêm da área de filtragem e validação do XML. Como o XML é usado como mecanismo de intercâmbio de dados, torna-se cada vez mais importante inspecionar, validar, depurar e proteger as transações XML.

A seguir, temos algumas das funções oferecidas pelo BIG-IP ASM para superar os desafios da segurança XML.

Modelos para validação XML

Com mais de vinte perfis diferentes para aplicativos, linguagens de script e analisadores XML, o BIG-IP ASM tem a capacidade de proteger os aplicativos assim que é implementado. Os mecanismos de distribuição como o RSS feed, Outlook Web Access e aplicativos corporativos de segundo plano como o Oracle e o SAP agora podem receber a mesma proteção, garantindo que os dados cheguem até onde precisam ir, de forma rápida e segura. Entre os modelos incluídos, estão:

- RSS 2.0 Feed Server
- SharePoint 2007
- Outlook Web Access
- Analisadores XML como Xerces, libxml2 e Oracle Application Server
- Portal de Aplicativos Oracle
- Python, Ruby, JavaScript e PHP

À medida que mais aplicativos de desktops podem receber e processar XML diretamente, torna-se cada vez mais importante garantir que a entrada e saída de dados em XML de e para aplicativos baseados na web sejam bem formadas e tenham os elementos necessários. Com o Outlook 2007, Internet Explorer 7 e Firefox entre os aplicativos que podem agregar feeds RSS para os usuários finais, garantir que os dados XML estão "limpos" se tornou uma parte importante na conquista e manutenção da confiança desses usuários. Se os usuários não confiam nos dados ou na maneira como você os distribui, vão procurar o que precisam em outro lugar, e isso nunca é bom.

Aqui entram os modelos de aplicativos do BIG-IP ASM, com medidas de segurança XML específicas para aplicativos. Usando esses modelos para criar um perfil de aplicativos, a proteção básica desses tipos de servidores e plataformas de aplicativos podem ser implementada com pouco mais do que alguns cliques do mouse do administrador. De maneira rápida e eficiente, os modelos do BIG-IP ASM podem ajudar a impedir a maioria dos ataques de validação XML comuns. Se os vetores mais rápidos para um sistema estiverem bloqueados, a maioria dos agressores escolherá outro alvo. O resultado geral é que os aplicativos e os dados permanecem seguros e disponíveis, com menos esforço.

Validação DTD

Ampliando o sistema de análise existente no BIG-IP ASM, a versão 9.4.2 expande suas capacidades ao território da validação de conteúdo XML de acordo com Definições de Tipos de Documentos (DTD) locais e remotas. Ao importar DTDs ou Web Services Description Language (WSDL), o BIG-IP ASM pode verificar a validação no conteúdo XML no tráfego HTTP, bloqueando elementos desconhecidos ou indesejados e garantindo a validade do conteúdo, baseando-se no esquema. Além disso, as referências aos esquemas hospedados externamente podem ser controladas, garantindo a origem boa e conhecida dos esquemas processados e validados. A centralização do controle e validação de documentos DTD e WSDL reduz o risco para os usuários finais, caso um servidor de segundo plano seja comprometido e esses documentos sejam modificados para conduzir a um site malicioso.

A capacidade de validar as solicitações XML tanto pela formatação adequada como pelo uso correto dos elementos do esquema nas solicitações e respostas melhora a capacidade do BIG-IP para detectar o abuso e executar ações corretivas. Dois tipos de ataques orientados a DTD são mais comuns: A redefinição DTD e a Entidade Externa XML (XML eXternal Entity - XXE). Ambos ataques permitem ao analisador XML de um cliente, como aqueles encontrados no navegadores, permanecer sob o controle de outra pessoa. Como a gramática XML maliciosa poderia ser executada com os mesmos nomes de elementos usados por elementos legítimos, isso poderia contornar qualquer validação no próprio aplicativo, deixando a máquina do cliente aberta para vários níveis de comprometimento do sistema.

No caso do primeiro tipo de ataque, o DTD ou o esquema contém um link ou outra referência que chama um segundo DTD ou esquema, que é carregado e processado pelo analisador XML do cliente. O analisador avalia então essa segunda DTD como se fosse aquela solicitada inicialmente. Explorando a confiança do usuário na localização da primeira DTD, como um site de compras na Internet, a segunda DTD pode ser carregada, podendo causar problemas para a máquina do cliente.

Como os analisadores XML são integrados a muitos programas de uso comum, como navegadores da web e processadores de texto, esse tipo de ataque de redefinição pode ser devastador. O ataque de redefinição pode ser combatido com um tipo de validação do analisador XML. Infelizmente, as versões atuais do Firefox e do Internet Explorer não têm um analisador XML que valide documentos DTD e do esquema. Como resultado, cerca de 93% dos usuários da Internet são alvos em potencial para esse tipo de ataque, simplesmente porque decidiram usar o navegador Internet Explorer ou Firefox.ⁱⁱⁱ

Com o BIG-IP ASM, entretanto, toda a validação é feita antecipadamente, incluindo qualquer referências por links no DTD/esquema. Qualquer código malicioso presente no DTD/esquema é interceptado antes que alcance o analisador XML do cliente, evitando problemas que poderiam prejudicar a confiança do usuário em um site ou serviço.

O mesmo acontece com os ataques XXE. Bastante similares aos ataques de redefinição DTD, os ataques XXE são diferentes porque o DTD é simplesmente alterado ou tem elementos adicionados a ele, em vez da substituição completa que acontece na redefinição DTD. Mais uma vez, o sistema de validação do BIG-IP ASM examina a gramática XML apresentada pelo documento externo antecipadamente, seguindo o link HTTP embutido no código XML original, decompondo o código externo e fazendo a sua validação. Com as referências sendo checadas de

antemão, o potencial para ataques de Cross-Site Scripting em documentos XML, ou mesmo outros ataques mais perigosos, é imensamente reduzido.

Segurança e filtragem de operações WSDL

Documentos WSDL simultâneos, como muitos itens relacionados a serviços, podem ser um benefício ou um risco. As operações contidas em um documento WSDL permitem solicitações e recuperações flexíveis de dados como uma camada de abstração de interfaces de linguagens específicas. Com essa flexibilidade, também vem o risco de expor as operações de teste e depuração à rede externa, gerando riscos de indisponibilidade, instabilidade do sistema ou atividades maliciosas.

Como o DTD já mencionado, o WSDL também precisa ser validado de maneira semelhante. Garantir que uma gramática XML inválida (malformada) não gerará problemas é o primeiro passo para proteger os aplicativos. A segunda parte da proteção de aplicativos é mais difícil, pois envolve o equilíbrio entre segurança e uso.

No caso das WSDLs, algumas operações incluídas na WSDL podem não ser para uso público, como as que invocam resultados de testes de QA. Pode haver outras operações que devem somente ser usadas de certas maneiras, para impedir o consumo excessivo de recursos. Embora seja tentador negar a invocação externa da WSDL de um site, clientes e parceiros podem depender dos dados recuperados por aquela interface e, portanto, algumas permissões devem ser concedidas. Servidores de aplicativos como o BEA WebLogic geram uma definição WSDL de forma dinâmica para cada aplicativo hospedado. Para manter o equilíbrio, você precisa de supervisão.

Aqui entra o BIG-IP ASM para fornecer a segurança da distribuição de aplicativos. Usando a interface do BIG-IP ASM, a especificação de operações WSDL válidas pode ser feita de forma simples e granular.

Importando a WSDL diretamente para o BIG-IP ASM, você utiliza os benefícios do gerenciamento centralizado. E centralizar a imposição da WSDL garante que a WSDL válida não será sobrescrita por uma versão maligna, e que as operações habilitadas permanecerão consistentes em todos os servidores de segundo plano. Quando importadas, as operações do arquivo WSDL são exibidas como caixas de checagem na interface do BIG-IP ASM. Você quer negar acesso a certas operações? Basta desmarcá-las e aplicar o perfil ao aplicativo. É simples assim. Permitir que os usuários remotos invoquem as operações necessárias e garantir que as operações perigosas não estejam expostas ou possam ser enumeradas por um agressor ajuda a conter o risco (exposição) da infra-estrutura de segundo plano, mantendo a disponibilidade dos aplicativos e dos dados.

O equilíbrio entre uso e segurança está estabelecido e mantido: problema resolvido.

Parâmetros ajustáveis de validação de elementos

Pela descrição, essa função não parece particularmente inovadora. À semelhança das funções descritas, essa também se destaca ao ser inserida no contexto da resolução de problemas de alto risco em potencial. Bombas XML e Injeções de Transformação.^{iv}

Em resumo, as bombas XML exploram regras que exigem que as referências de entidades sejam expandidas para avaliação. As bombas XML adicionam entradas de entidades externas a um documento XML, normalmente incluindo uma definição DTD com essas entradas antes do elemento raiz do documento. Essas entidades

normalmente são numeradas de forma seqüencial e definidas e redefinidas de forma similar às variáveis de programação ou scripts.

Por exemplo, se a primeira entidade for "ABC" e tiver sido definida como "ABC!", a próxima entidade, "ABC2", seria definida como "&ABC; &ABC". As entidades subseqüentes seriam definidas com base no valor expandido da entidade anterior; "ABC3" é expandida para "&ABC, &ABC, &ABC, &ABC", quando as duas entidades "ABC2" são expandidas dentro da definição de "ABC2". Como os valores das entidades crescem rapidamente à medida que elas são expandidas ("ABC128" seria equivalente a 2×2^{127} entidades "ABC"), o resultado é a exaustão dos recursos de memória e processador, causando um desempenho ruim ou travamentos dos aplicativos. Um analisador XML pode ser vítima desse ataque mesmo se for instruído para não expandir as entidades, porque a expansão de entidades é uma ação válida e requerida para os documentos XML.

Um problema similar para a segurança XML são as injeções de transformação. Como as bombas XML, o objetivo é a negação de serviço, consumindo recursos da memória e do processador nas máquinas dos clientes. Os problemas de exploração das injeções de transformação ocorrem ao converter dados XML para outra forma ou apresentação. Como é baseado em regras, o ambiente XSLT (eXtensible Stylesheet Language Transformations) inclui funções de controle de fluxo como parte de seu conjunto de ferramentas de transformação de dados. Embora essas funções possam ser muito poderosas para executar funções repetitivas, como a conversão de dados XML para HTML, elas também podem ser usadas de forma maliciosa para criar loops infinitos que consomem recursos. Transformações redundantes também podem ser incluídas ("injetadas") nas instruções de transformação, causando o consumo de recursos. Quando o avaliador XML examina essas transformações redundantes, transformando os dados originais repetidamente sem modificá-los, ele deve alocar memória para manter o registro de cada instrução de transformação, mesmo que ela não resulte em uma ação.

O BIG-IP ASM pode cuidar diretamente desses problemas. Os limites na expansão máxima de entidades e o número de recursão de níveis de entidades estão entre os mais de 15 parâmetros que podem ser ajustados pela interface gráfica, contendo ou anulando os efeitos de uma bomba XML. A profundidade dos pares de elementos-filho, a quantidade máxima de dados contidos em um par de elementos e o tamanho máximo de um documento XML também podem ser definidos para mitigar os efeitos de ataques de injeção de transformação.

Três níveis integrados de segurança (alto, médio e baixo) oferecem valores básicos para os parâmetros de validação, ajudando a criar políticas que podem ser aplicadas imediatamente para proteger dados e aplicativos. Uma política mais granular pode ser criada e aplicada, tanto manualmente como com o Real Time Policy Builder, caso necessário.

Conclusão

Embora cada uma das funções detalhadas acima sejam apresentadas como funções separadas, o poder e a flexibilidade do BIG-IP ASM é demonstrado pelos perfis de aplicativos que podem combinar aspectos das diferentes funções do firewall XML. A capacidade de criar políticas personalizadas para qualquer aplicativo baseado em XML e aplicá-las em um ponto central de administração significa que os administradores podem agora implementar políticas de segurança no nível da companhia, não apenas no nível específico de um aplicativo. Graças à sua localização na rede, o BIG-IP ASM 9.4.2 tem a capacidade de remover os riscos da distribuição de aplicativos.



Ao adotar uma abordagem holística da segurança de distribuição de aplicativos, as funções do BIG-IP ASM oferecem grande facilidade na criação, teste e implementação de políticas. Ao aplicar as políticas predefinidas ou usar o Real Time Policy Builder para criar políticas mais específicas, o BIG-IP ASM pode implementar a segurança de distribuição de aplicativos de forma muito mais rápida e precisa do que seus antecessores.

A segurança precisa ser ampliada além da Web 2.0. Embora a Web 2.0 seja focada em novos meios de integrar e apresentar dados, a proteção desses dados também exige uma abordagem integrada, não apenas um dispositivo dedicado a uma pequena parte do processo de distribuição dos dados aos clientes. Como parte da estratégia integrada de segurança de distribuição de aplicativos da F5, o BIG-IP ASM tem as funções, flexibilidade e força necessários para levar a segurança de aplicativos ao próximo nível.

i Para informações adicionais sobre TMOS, o Real-Time Policy Builder e outros aspectos da arquitetura do BIG-IP ASM, visite www.f5.com.

ii Para informações adicionais sobre DTDs e WSDLs, visite w3.org.

iii W3Schools.com, "*Browser Statistics*," julho de 2007.

iv Uma boa visão geral sobre bombas XML pode ser encontrada no site *Search Software Quality* da Tech Target.