# Ameaças XML

Aqui está um breve resumo das ameaças à segurança da web service XML. Eles podem ser classificados em três grandes categorias com base no impacto nos negócios das ameaças:

**Negação de Serviço** - Desativar ou desacelerar um web service para que as solicitações de serviço válidos, sejam negados.

**Acesso não autorizado** - Acesso não autorizado a um web service ou seus dados.

**Comprometimento do sistema -** Corrompendo o serviço web ou os servidores de hospedagem.

Note que os ataques individuais podem ser combinados e utilizados como parte de um complexo esforço de recolha de dados ou fissuras, aumentando assim a ameaça.

**Ataque DoS**

Um serviço Web desprotegido é vulnerável a uma ampla gama de Denial of Service (Ataque DoS), que podem degradar ou até mesmo desativar serviços prestados aos seus usuários legítimos. Essas ameaças incluem DoS tradicionais, como DoS IP na camada de transporte, bem como Denial of Service XML (XDoS).

Ataques às mensagens XDoS incluem:

• **Cargas Jumbo** - Encaminhar uma mensagem XML muito grande, que pode ter centenas de megabytes ou gigabytes de tamanho para esgotar a memória e CPU no sistema de destino.

• **Elementos recursivo** - Mensagens XML maliciosas podem ser usadas para forçar a expansão de entidades recursiva ou processamento repetido para esgotar os recursos do servidor.

• **MegaTags -** Também conhecido como Jumbo, o envio de outra forma válida de mensagens XML com nomes de elementos excessivamente longos, podem levar à saturação mais grave do buffer.

• **Análise coercitivo -** O envio de uma mensagem XML que é especialmente construído para dificultar o acesso aos aos recursos da máquina, similar a elementos recursivos, o que é especialmente um problema se você estiver usando código legado para analisar os dados enviados através de uma mensagem XML.

• **Chave Pública DoS** - Utilizando a natureza assimétrica de operações de chave pública para forçar o esgotamento de recursos do receptor através da transmissão de uma mensagem com um longo número de comprimento de chave, com assinaturas digitais computacionalmente caras.

Ataque de Mensagens Múltiplas XDoS incluem:

• **Excesso XML -** Enviar milhares de mensagens de outra forma benigna por segundo para amarrar o seu serviço web. Este ataque pode ser combinado com a repetição de ataque para contornar XdoS mensagens de autenticação e único para aumentar seu impacto.

• **Recursos Hijack -** Envio de mensagens que bloqueiam os recursos no servidor de destino como parte de uma operação nunca concluída.

**Acesso não autorizado**

Utilizando o web service para concluir o que foi projetado, mas sem a devida permissão, é outra categoria comum de ataques. Os atacantes podem ter acesso a dados confidenciais, ou executar ações com impacto grave nos negócios, tais como alterar ou subrescrever dados.

Acesso não autorizado pode ser resultado de falhas de identificação de pares, identificação e autenticação de origem de dados podem envolver acesso falso como usuário falso e incluem:

• **Ataque Dicionário -** Também conhecido como adivinhação de senha, adivinhar a senha de um usuário válido usando uma pesquisa de força bruta através de palavras do dicionário.

• **Mensagem Falsificada** - Fingindo ser uma mensagem de usuário válido, utilizando ataque man-in-the-middle para ganhar uma mensagem válida e modificá-la, encaminhando uma mensagem diferente.

• **Replay Atack –** Reencaminhar uma mensagem previamente válida como efeito malicioso. Outras melhorias incluem a reprodução de partes da mensagem, onde apenas partes da mensagem (como o token de segurança) são repetidos.

Outra classe de ataques em web services XML, com um impacto direto sobre a integridade de dados, nas respostas web services, solicitações ou bancos de dados subjacentes:

• **Falsificação de Mensagem –** Modificando parte de uma solicitação ou resposta em vôo, mais perigoso quando não detectado, menos comumente conhecido como "Alteração de Mensagem". Para mensagens com anexos, alteração de anexos, uma variação desse ataque.

• **Data Tempering -** Explorando a fraqueza no mecanismo de controle de acesso que permite fazer chamadas não autorizadas para web services, para alterar os dados.

Os ataques que violam a confidencialidade de dados e, possivelmente, obter acesso não autorizado aos serviços:

• **Mensagem Snooping –** Conhecido como subconjunto de ataque man-in-the-middle, este é um ataque direto à privacidade de dados, analisando a totalidade ou parte do conteúdo de uma mensagem. Isso pode acontecer com mensagens transmitidas criptografadas, mas armazenadas em claro, ou descriptografia de mensagens, devido a chave roubada ou criptoanálise.

• **Xpath Injection -** A expressão Xpath Injection, na lógica do aplicativo, também chamado de XQuery ou XSLT Injection. Novas modificações incluem blind XPath Injection, o que reduz o conhecimento necessário para montar o ataque.

• **SQL Injection -** Inserir SQL em XML para obter dados adicionais, além do que o serviço foi projetado para retornar.

• **Enumeração WSDL** - Examinar os serviços listados em WSDL para ter acesso a serviços não listados.

• **Desvio de Roteamento –** Utilizando roteamento SOAP para acesso a web services internos.

**Comprometimento do sistema**

Considerando que os ataques de acesso não autorizados permitam acesso inválidos a web service, ataques que comprometem o sistema vão um passo além. Eles podem fazer com que o web service em si ou o servidor que hospeda o serviço ser comprometido, e a queda sob o controle de um ataque.

Ataque ao sistema que alteram o comportamento da aplicação XML incluem:

• **Envenenamento do esquema** - A substituição do esquema XML válido como inválido. Isto pode ser utilizado para contornar a validação do esquema ou criar uma mensagem única XDoS por buscar um esquema de grandes dimensões a partir de um servidor lento.

• **Morphing Malicioso -** Causando uma saída web service para um formato não intencional.

Ataque Sistema ataques de compromisso que o controle de ganho do servidor incluem:

• **Incluir malicioso -** Também chamado ataque entidade externa XML (XXE), causando um web service para incluir dados externos inválidos na saída ou retornar os arquivos privilegiados do servidor de sistema. Por exemplo, utilizando o arquivo incorporado, URLs para retornar arquivos de senhas Unix ou outros dados privilegiados no ataque.

• **Violação de espaço de memória -** Realizado através de stack overflow, estouro de buffer ou erro Heap, permite execução de código arbitrário fornecido pelo ataque com permissões de processo de hospedagem.

• **Encapsulamento XML** - Comando de incorporação do sistema na carga XML, por exemplo, a tag CDATA.

• **Virus XML -** Ou X-Virus, utilizando SOAP com anexos ou mecanismos de fixação para transmitir outros executáveis maliciosos, como vírus ou worms.

O WebSphere DataPower XI52 oferece proteção contra essas e outras ameaças XML. Além de um firewall XML altamente seguro, que inclui o quadro AAA (Autorização, Autenticação e Auditoria) para controle de acesso, segurança de campo, serviço de virtualização e roteamento baseado em conteúdo XML - recursos combinados que oferecem tanto proteção contra ameaças e segurança de conectividade.