



Análise de Vulnerabilidade

Documento Confidencial

RE 040326-01-01 – RV 00

São Paulo, 26 de Março de 2004



Índice

Resumo Executivo.....	3
Política de Privacidade	5
Terminologia	6
Endereços Analisados	9
Portas Abertas Detectadas	10
Vulnerabilidades Detectadas	11
Descrição Técnica.....	12

Resumo Executivo

Cliente: NX Security

Número do Documento: 040326-01-01

Data da Análise: 24 de Março de 2004

Endereço IP/DNS Utilizado: 10.10.10.1

Total de Vulnerabilidades: 3

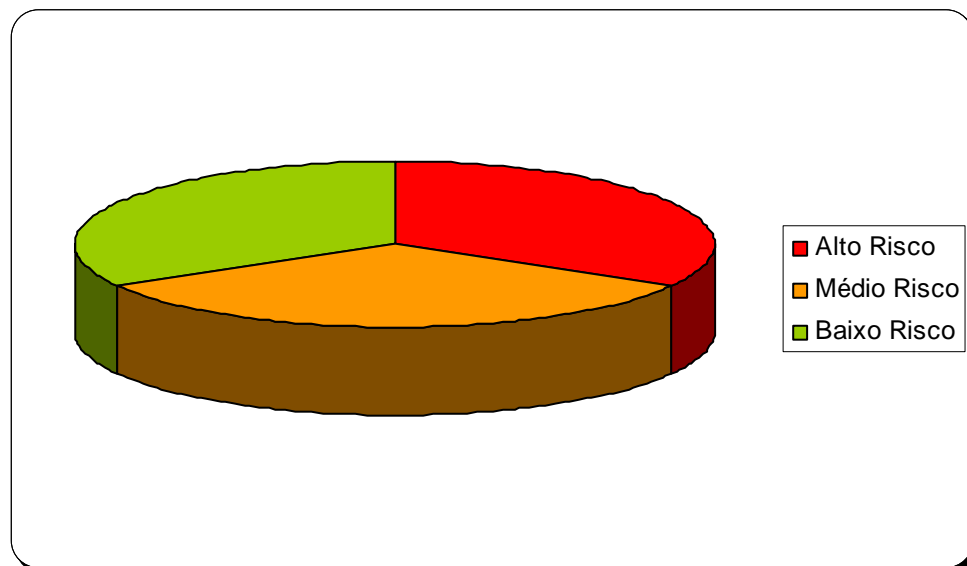
Este documento descreve os resultados obtidos através do serviço de Análise de Vulnerabilidade, Teste de Vulnerabilidade e Teste de Invasão prestados pela NX Security junto ao cliente mediante a assinatura de um Termo de Confidencialidade. O escopo do serviço é auditar e analisar internamente os sistemas e/ou recursos especificados pelo cliente dentro de seu ambiente local de rede (LAN).

Durante o processo de análise, foram encontradas 3 vulnerabilidades nos endereços indicados pelo cliente que estão listados na seção Endereços Analisados. Dessas 3 vulnerabilidades 1 é considerada de alto risco, 1 é de médio risco e 1 de baixo risco.

Alto Risco
1 (34%)

Médio Risco
1 (33%)

Baixo Risco
1 (33%)





A vulnerabilidade considerada como alto risco, é uma falha na biblioteca ASN.1 utilizada nos sistemas Windows, com esta vulnerabilidade um usuário pode executar comandos remotamente na máquina. A Microsoft já disponibilizou uma correção para esse problema.

É necessário que as atualizações do sistema Windows seja feita com urgência, evitando dessa forma que um usuário mal intencionado faça proveito da vulnerabilidade detectada e amplamente divulgadas na Internet.

A seção Detalhes Técnicos provem informações detalhadas sobre os problemas detectados bem como suas correções e melhores práticas para o ambiente. Caso haja o não entendimento de algum termo técnico apresentado neste relatório, suas definições poderão ser encontradas na seção Terminologia.



Política de Privacidade

As informações obtidas durante os serviços prestados pela NX Security para o cliente incluindo seus recursos, procedimentos e sistemas, é informação privilegiada sendo tratada como confidencial. A NX Security compromete-se em manter com extremo sigilo todas as informações contidas neste documento. Não será comentado e/ou revelada nenhuma informação a terceiros sem uma plena autorização por escrito do cliente.

Este documento descreve o acordo realizado entre a NX Security junto ao cliente mediante a assinatura de um Termo de Confidencialidade, concedendo a autorização de analisar a segurança da rede de dados utilizando-se de diversos meios eletrônicos. A autorização é concedida para um determinado número de endereços eletrônicos indicados pelo cliente e listados na seção Endereços Analisados deste documento. Os nomes de produtos citados neste documento são marcas registradas de suas respectivas companhias onde estão sujeitas à mudanças sem o prévio aviso e não deverão ser interpretadas como um compromisso pelo fabricante e/ou fornecedor.

Terminologia

A NX Security utiliza uma base de dados com mais de 2.000 vulnerabilidades. Cada uma dessas vulnerabilidades são classificadas por um nível de risco, que é a severidade do problema de segurança ou a probabilidade que uma pessoa mal intencionada pode explorar esta vulnerabilidade. Este documento utiliza determinadas terminologias que podem inicialmente não ser familiar, as informações abaixo descrevem cada nível de risco e algumas terminologias técnicas utilizadas neste documento.

- **Definição dos Fatores de Risco**

- Alto Risco**

Todas as ameaças de segurança que possam comprometer a integridade dos dados, expor informações confidenciais ou ser utilizadas para indisponibilizar os sistemas da empresa são consideradas de alto risco. Estes tipos de ameaças devem ser tratadas com prioridade e são fáceis de serem exploradas.

- Médio Risco**

São ameaças de segurança que podem abrir seu sistema para pessoas não autorizadas, expor dados, arquivos e informações ou causar algum tipo de paralisação, normalmente em alguma aplicação específica são consideradas de médio risco. Normalmente, mas não sempre, são mais complexas para serem exploradas sendo necessário uma atenção alta em sua correção.

- Baixo Risco**

Esta classificação de ameaça de segurança é utilizada para problemas que normalmente não podem ser utilizadas independentemente para ganhar acesso não autorizado aos dados da empresa ou comprometer um sistema, porém, esse tipo de ameaça normalmente é combinada a outro tipo de informação para explorar os sistemas.

- **Definição das Terminologias**

- CGI**

Common Gateway Interface. Uma estrutura padrão e protocolo utilizado para executar programas através de um servidor web. Por exemplo, um portal de e-commerce que processa cartões de crédito provavelmente utiliza CGI.

- CVE/CAN**

Common Vulnerabilities and Exposures / CANDidate. Uma lista de nomes padronizada para vulnerabilidades e outras exposições na área de segurança da informação.

DoS	Denial of Service. DoS é um tipo de ataque a redes que procura indisponibilizar servidores, equipamentos de rede ou aplicações.
DNS	Domain Name System/Service. É o protocolo utilizado na Internet para traduzir nomes de domínios em endereços da Internet. Por exemplo, o endereço www.nxsecurity.com é traduzido para 200.155.25.4.
Endereço IP	É a representação numérica de endereço de um computador na Internet.
Exploit	Ferramenta criada por Hackers/Crackers para explorar vulnerabilidades em sistemas.
Fingerprint	Nome dado a uma técnica utilizada para identificar quais serviços, protocolos, sistemas operacionais estão ativos na rede.
Firewall	É um sistema designado para prevenir o acesso não autorizado de uma rede ou para uma outra rede. Os Firewalls podem ser implementados tanto em software como em hardware ou com a combinação de ambos. Firewalls normalmente são utilizados para prevenir o acesso não autorizados de usuário da internet a uma rede privada de computadores.
MTA	Mail Transport Agent. Programa utilizado para processar mensagens de e-mails e seus protocolos. Por exemplo, Exchange e Sendmail.
Porta	Uma interface de rede de computador é dividida em diversos canais, cada canal é chamado de "Porta". A porta é utilizada pelo hardware ou por um software específico para fazer requisições na rede. Por exemplo, um servidor web utiliza a porta 80 para aceitar conexões dos navegadores dos usuários.
Port Scan	É o processo utilizado para determinar quais portas estão ativas em um sistema. O PortScan não determina qual protocolo ou aplicação específica esta sendo utilizado, apenas verifica quais estão abertas ou fechadas.
Protocolo	É o padrão da regulamentação de transmissão de dados entre computadores. Por exemplo, um servidor de e-mail utiliza determinados protocolos para que haja uma comunicação entre si.
Rede/Network	Grupo de computadores ou equipamentos conectados entre si. Uma LAN (Local Área Network) é um exemplo de rede.
Roteador	Equipamento responsável na transmissão de pacotes de dados entre redes de computadores.



Serviço	Determinada aplicação oferecida pelo servidor. Por exemplo, Um servidor web oferece o servidor de prover páginas na Internet para um navegador web.
Servidor	Computador responsável para prover serviço(s) para outros computadores que estão conectados a ele diretamente ou através de uma rede.
SSL	Secure Sockets layer. Um Protocolo designado a prover comunicação encriptada e segura na Internet entre o servidor e um computador. O SSL é normalmente utilizado em sites de e-commerce e bancos via Internet. Porém, o SSL não fornece segurança após o envio dos dados.
TCP/IP	Transmission Control Protocol/Internet Protocol. Conjunto de dados de rede e comunicação de protocolos para comunicação entre computadores, utilizado como padrão para transmissão de dados em uma rede.
Vírus	Um programa ou parte de códigos de programação que ficam armazenados no computador sem consentimento do usuário, podendo se replicar automaticamente contaminando outras máquinas ou fornecer informações para um usuário mal intencionado.
Vulnerabilidade	Uma falha de programação/design em determinado software ou aplicação permitindo executar comandos não permitidos em um sistema.



Endereços Analisados

Esta seção descreve os endereços IP e os nomes de domínios que foram autorizados a serem analisados pela equipe da NX Security conforme descrito na Política de Privacidade.

Endereço IP	Endereço de Domínio	Sistema Operacional
200.200.200.200	www.nxsecurity.com	Windows 2000 Server

Portas Abertas Detectadas

Esta seção descreve as portas encontradas nos endereços analisados pela NX Security. Cada porta não representa necessariamente um risco, porém podem ser um ponto de entrada para um atacante. Aconselhamos que sejam expostos somente serviços necessários diminuindo dessa forma o risco de exposição do sistema. Os serviços apresentados abaixo em cada porta, são suas definições padrões, não sendo necessariamente sua atual aplicação.

Endereço IP	Porta	Protocolo	Serviço
200.200.200.200	21	TCP	FTP
	25	TCP	SMTP
	80	TCP	HTTP
	443	TCP	HTTPS

Vulnerabilidades Detectadas

Esta seção descreve as vulnerabilidades detectadas durante a análise realizada pela NX Security. Abaixo, as vulnerabilidades são resumidas com seu título, grau de risco e entrada CVE, veja sua descrição:

Título: Nome dado a vulnerabilidade podendo ser na língua portuguesa ou inglesa.

Risco: Grau de risco podendo ser Alto, Médio e Baixo conforme descrito na seção Terminologia.

CVE: Orgão Internacional responsável por padronizar vulnerabilidades conhecidas publicamente. Para obter maiores informações sobre a vulnerabilidade descrita, clique no número de referencia do CVE/CAN.

<u>CVE</u>	<u>Risco</u>	<u>Título</u>
CAN-2003-0818	Alto	Vulnerabilidade na biblioteca ASN.1
CAN-2001-0500	Médio	Filtro .IDA ISAPI mapeado
CAN-1999-0497	Baixo	Acesso anônimo ao servidor FTP

Descrição Técnica

Esta seção descreve os detalhes das vulnerabilidades detectadas durante o processo de análise realizada pela NX Security, onde está dividida em sub-seções de Vulnerabilidades de Alto Risco, Vulnerabilidades de Médio Risco e Vulnerabilidades de Baixo Risco. As informações desta seção inclui uma descrição por completo do problema detectado, a forma de correção, os dados coletados através da vulnerabilidade, os endereços afetados e sua entrada CVE.

- **Vulnerabilidades de Alto Risco**

Nome:	Vulnerabilidade na biblioteca ASN.1
Descrição:	Foi detectado a ausência do patch que corrige a vulnerabilidade na biblioteca ASN.1 utilizada em alguns serviços do Microsoft Windows. Esta vulnerabilidade permite um usuário mal intencionado executar comandos remotamente no servidor como usuário SYSTEM.
Solução:	- Aplique a correção disponibilizada pela Microsoft no boletim MS04-007; URL: http://www.microsoft.com/technet/security/bulletin/ms04-007.msp
CVE:	CAN-2003-0818
Dados Obtidos:	-
Endereços Afetados:	www.nxsecurity.com

- Vulnerabilidades de Médio Risco

Nome:	Filtro .IDA ISAPI mapeado
Descrição:	Foi detectado no servidor o filtro ISAPI mapeado, este filtro possui algumas vulnerabilidades, entre elas ganho de acesso remoto ao servidor, a Microsoft recomenda que desabilite este e outros filtros que não estejam sendo utilizados.
Solução:	- Remova o filtro .ida nas configurações do IIS; - Utilize o URLScan da Microsoft;
CVE:	CAN-2001-0500
Dados Obtidos:	-
Endereços Afetados:	www.nxsecurity.com

- Vulnerabilidades de Baixo Risco

Nome:	Acesso anônimo ao servidor FTP
Descrição:	Foi detectado que o servidor FTP possui o acesso anônimo habilitado. Caso não esteja sendo utilizado é aconselhado desabilitar esta função, evitando dessa forma futuros problemas.
Solução:	- Desabilite o acesso anônimo ao servidor FTP;
CVE:	CAN-1999-0497
Dados Obtidos:	-
Endereços Afetados:	www.nxsecurity.com