



NX Express

NX Express is a perfect solution for organizations reliant on the Internet for transactions or operations. Providing coverage of information security risks and exposures, **NX Express** facilitates all stages of risk management life-cycle. By evaluating the functionality of an application, unnecessary points of exposure can be identified and effectively managed. Through a continuous process of analysis, threats can be identified and mitigated before they become serious incidents that impact operations and the bottom line.

Solutions from **NX Security** empower network managers to safeguard their information infrastructures. **NX Express** audits network assets, providing clear and precise reports that pinpoint real concerns and effective means for risk remediation.



The screenshot displays a report interface with the following sections:

- Resumo Executivo:** Client: nx security - teste e instalação; Número de Documento: 0940219-05; Data de Análise: 07 de janeiro de 2004; Endereço IP/URL Utilizado: 200.200.200.200; Total de Vulnerabilidades: 3.
- Descrição Técnica:** Esta seção descreve os detalhes das vulnerabilidades detectadas durante o processo de análise realizado pelo 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 incluem uma descrição por completo do problema detectado, a forma de corrigir, os dados coletados através de vulnerabilidade, os endereços afetados e sua entrada CVE.
- Vulnerabilidades de Alto Risco:** Nome: Servico Padrao Utilizado; Descrição: Foi detectado que os equipamentos de rede utilizam senhas padrão fornecidas pelos fabricantes. Com isso um usuário mal intencionado pode acessar, modificar e alterar as configurações dos equipamentos; Solução: - Desabilitar as senhas padrão pelos fabricantes; - Criar uma política de senhas fortes; CVE: [CVE-1999-0508](#); Dados Origens: Senha de equipamento Cisco; Ibmcc; Cisco; Emulac; Cisco.
- Vulnerabilidades Detectadas:** Esta seção descreve as vulnerabilidades detectadas durante a análise realizada pelo 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 inglês.
Risco: Grau de risco podendo ser Alto, Médio e Baixo conforme descrito na seção Terminologia.
CVE: Órgão Internacional responsável por padronizar vulnerabilidades conhecidas publicamente. Para obter maiores informações sobre a vulnerabilidade descrita, clique no número de referência do CVE/CAN.
Table with 3 columns: CVE, Risco, Título.
Row 1: CVE-1999-0508, Alto, Servico Padrao Utilizado.
Row 2: CVE-1999-0517, Médio, Servico de SMTP habilitado.
Row 3: -, Baixo, Servicos de gerenciamento habilitados.
- Gráfico de Vulnerabilidades:** Um gráfico de pizza mostra a distribuição das vulnerabilidades por nível de risco: Alto Risco (33.33%), Médio Risco (66.67%) e Baixo Risco (0.00%).

NX Enterprise can provide real and lasting value to information security initiatives - through expert audits of the firm's Internet footprint, network DMZ, FTP, WEB and MAIL SERVERS, FIREWALL, IDS, IPS, ROUTERS, and all other network components. Features include:

- ✓ Comprehensive assessments – addressing over 8,000 vulnerabilities
- ✓ Powerful modes of operation, including Passive Vulnerability Assessment and Penetration Test
- ✓ Technical, Managerial and Didactic reports, detailing risk severity and expert recommendations for risk elimination or management
- ✓ Security analysis of network perimeter and public facing servers and services
- ✓ Analysis of web-based applications, including virtual shops, database environments and bespoke extranet infrastructures
- ✓ CVE Compatible: worldwide standard for identification and description of security vulnerabilities
- ✓ SANS Top-20: focused sub-set of the most critical threats
- ✓ Team technique specialized in better research and development of practical
- ✓ Supported by a dedicated team of vulnerability researchers, providing real-time signature updates and value-added features
- ✓ Backed by the **NX Security Incident Response Team**
- ✓ Integrated with **NX Security Alert**

Contact us today for a no-obligation consultation on how **NX Security** can benefit your enterprise.

Centro Empresarial Paulista – Av. Paulista 2300, Andar Pilotis
CEP 01310-300 - São Paulo - SP - Brazil
Tel.: +55 11 6847-4941 - Fax: +55 11 6847-4550
Email: comercial@nxsecurity.com