University of M'sila
Faculty of Mathematics and Computer Science
Department of Computer Science
Master's in Networks& TIC

Network v[illegible]erability

Prepared and presented by:
SAOUDI Lalia
2024-2025

1. What is a Network Vulnerability?

- A network vulnerability is a weakness or flaw in a network's hardware, software, protocols, or security policies that an attacker can exploit to gain unauthorized access, disrupt service, or steal data.

What is a erability

- In computer security, a vulnerability or flaw is a weakness in the computer system that allows an attacker to compromise the confidentiality, integrity, and availability of data or IT resources.

Common Source Network Vulnerabilities:

- **Unpatched Software:** Failing to apply security updates.
- **Misconfigurations:** Default passwords, open ports, poorly configured services.
- **Weak Network Architecture:** Lack of segmentation, flat networks.
- **Insecure Protocols**: Using unencrypted services like Telnet or FTP.
- **Human Factor:** Phishing, poor password hygiene

Types of Vulnerability alerts

1)Vendor Security Advisories

1) Format: Technical bulletins from software/hardware vendors
2) Examples: Microsoft Security Bulletins, Cisco Security Advisories
3) Content: Affected versions, impact, workarounds, patches

2)Cert advisories

1) Source: Computer Emergency Response Team Coordination Center
2) Authority: Government-backed technical analysis
3) Focus: Critical widespread vulnerabilities

Types of Vulnera y alerts

1)3)CVE : The Common Vulnerabilities and Exposures (CVE) system was created by The MITRE Corporation ,

2) The CVE catalog is more like a dictionary than a CVE database. It provides one name and one description for each vulnerability or exposure

CVE Website: https://cve.mitre.org

4)NVD (National Vulnerability Database) NVD: Enhances CVE data with:

- CVSS severity scores
- Patch information
- Impact ratings
- Search capabilities

Vulnerability key concepts:

C**VSS (Common Vulnerability Scoring System)**: A framework for rating the severity of vulnerabilities (e.g., CVSS 9.8 = Critical).

Zero-Day Vulnerability: A flaw unknown to the vendor, with no available patch.

Computer Emergency Response Team (CERT)

Computer Emergency Response Team (CERT) is an expert group that handles computer security incidents by detecting, responding to, and preventing cyberattacks. These teams, also known as (CSIRTs), provide guidance, share information, and help organizations or communities improve their cybersecurity posture through both proactive and reactive measures.

Computer Emergency Response Team (CERT)

Computer Emergency Response Team

https://www.educert.ma/index.php/form-contact.html

EDUCERT
Security Incident Response for Education

HOME | SERVICES | CONSTITUENCY | POLICIES | REPORT AN INCIDENT | CONTACT | SECURITY ALERTS | ADVISORIES

You are here: Home // Report an Incident

To Report a Security Issue, please fill in the form above:

First Name*
Last Name*
E-mail*
Phone Number
University/Insitution*
Please provide a short description of the incident and impact*

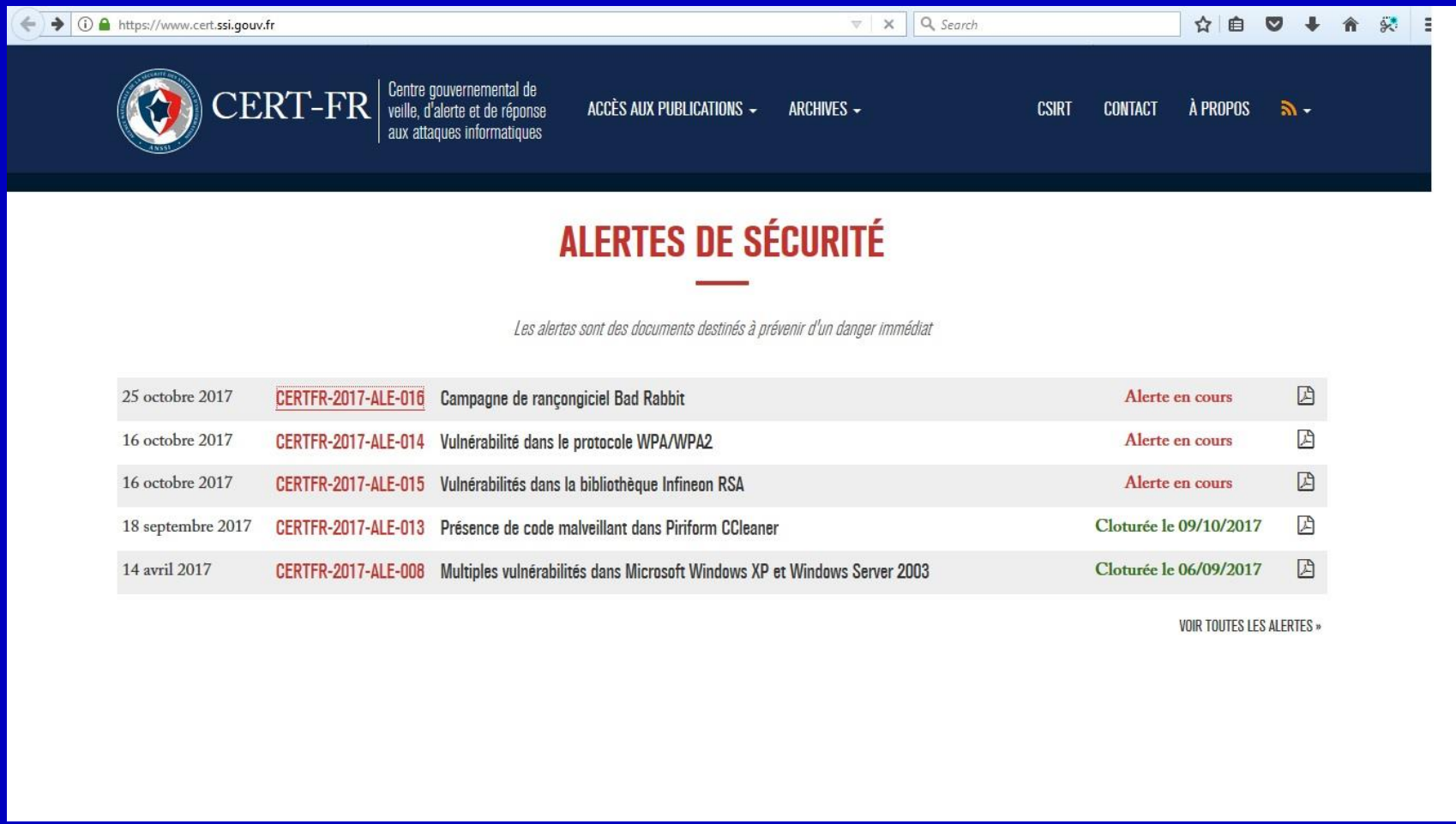
SECURITY NEWS

Cisco SocialMiner Cross-Site Scripting Vulnerabili...
A vulnerability in the web-based management interface of Cisco SocialMiner could allow an unauthenticated, remote attack...
2 days ago

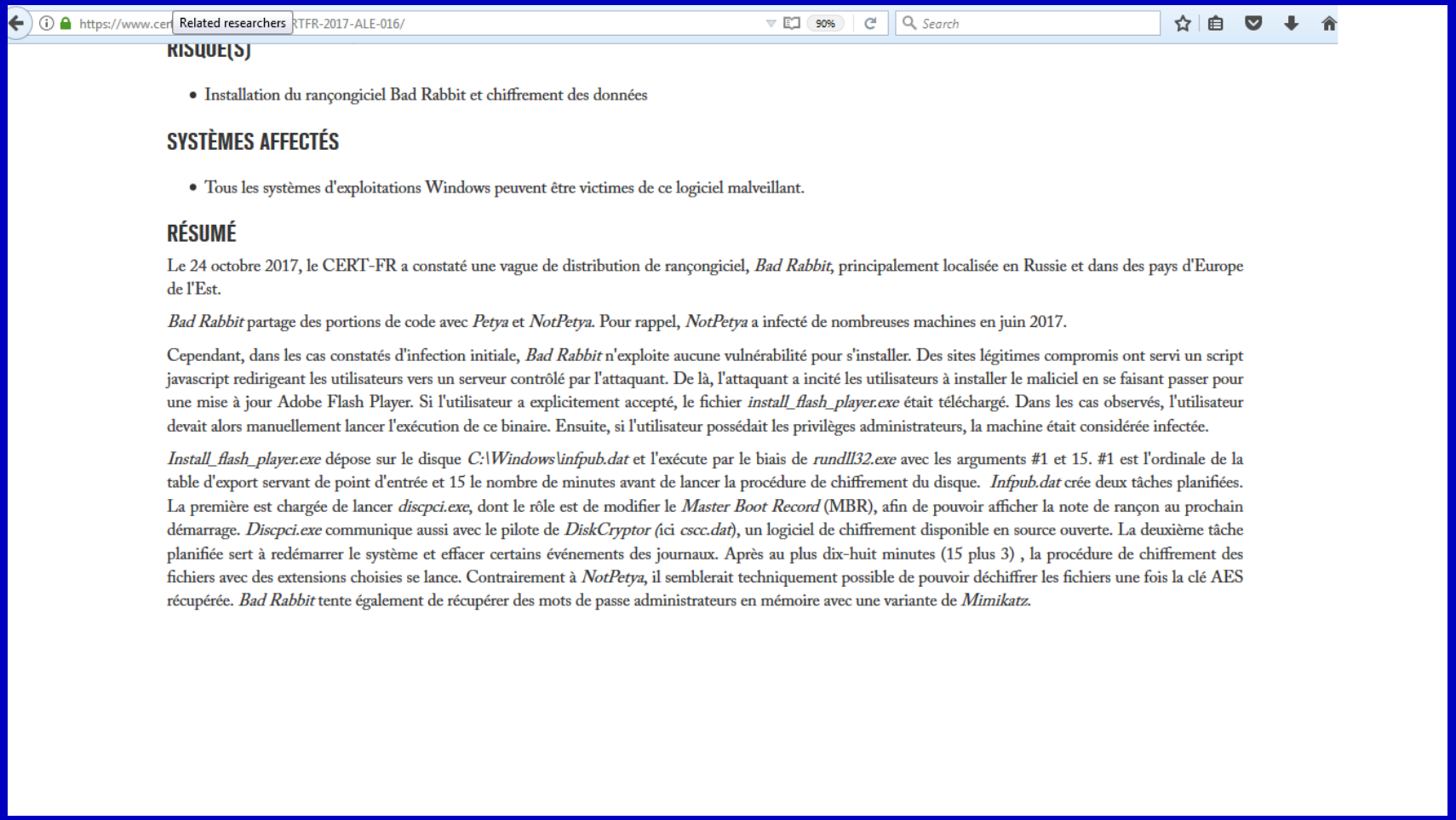
Cisco Wireless LAN Controller Software Privilege E...
A vulnerability in the authentication and authorization checking mechanisms of Cisco Wireless LAN Controller (WLC) Softw...

Computer Emergency Response Team

Computer Emergency Response Team



Vulnerability report example



https://www.cer Related researchers RTFR-2017-ALE-016/ 90% Search

RISQUE(S)

- Installation du rançongiciel Bad Rabbit et chiffrement des données

SYSTÈMES AFFECTÉS

- Tous les systèmes d'exploitations Windows peuvent être victimes de ce logiciel malveillant.

RÉSUMÉ

Le 24 octobre 2017, le CERT-FR a constaté une vague de distribution de rançongiciel, *Bad Rabbit*, principalement localisée en Russie et dans des pays d'Europe de l'Est.

Bad Rabbit partage des portions de code avec *Petya* et *NotPetya*. Pour rappel, *NotPetya* a infecté de nombreuses machines en juin 2017.

Cependant, dans les cas constatés d'infection initiale, *Bad Rabbit* n'exploite aucune vulnérabilité pour s'installer. Des sites légitimes compromis ont servi un script javascript redirigeant les utilisateurs vers un serveur contrôlé par l'attaquant. De là, l'attaquant a incité les utilisateurs à installer le maliciel en se faisant passer pour une mise à jour Adobe Flash Player. Si l'utilisateur a explicitement accepté, le fichier *install_flash_player.exe* était téléchargé. Dans les cas observés, l'utilisateur devait alors manuellement lancer l'exécution de ce binaire. Ensuite, si l'utilisateur possédait les privilèges administrateurs, la machine était considérée infectée.

Install_flash_player.exe dépose sur le disque *C:\Windows\infpub.dat* et l'exécute par le biais de *rundll32.exe* avec les arguments #1 et 15. #1 est l'ordinale de la table d'export servant de point d'entrée et 15 le nombre de minutes avant de lancer la procédure de chiffrement du disque. *Infpub.dat* crée deux tâches planifiées. La première est chargée de lancer *discpci.exe*, dont le rôle est de modifier le *Master Boot Record* (MBR), afin de pouvoir afficher la note de rançon au prochain démarrage. *Discpci.exe* communique aussi avec le pilote de *DiskCryptor (*ici *cscc.dat*), un logiciel de chiffrement disponible en source ouverte. La deuxième tâche planifiée sert à redémarrer le système et effacer certains événements des journaux. Après au plus dix-huit minutes (15 plus 3) , la procédure de chiffrement des fichiers avec des extensions choisies se lance. Contrairement à *NotPetya*, il semblerait techniquement possible de pouvoir déchiffrer les fichiers une fois la clé AES récupérée. *Bad Rabbit* tente également de récupérer des mots de passe administrateurs en mémoire avec une variante de *Mimikatz*.

Vulnerability report example

https://www.cert.ssi.gouv.fr

Search

AVIS DE SÉCURITÉ

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir

3 novembre 2017	CERTFR-2017-AVI-391	Multiples vulnérabilités dans OpenSSL
3 novembre 2017	CERTFR-2017-AVI-390	Multiples vulnérabilités dans le noyau Linux de SUSE
2 novembre 2017	CERTFR-2017-AVI-389	Multiples vulnérabilités dans les produits Cisco
2 novembre 2017	CERTFR-2017-AVI-388	Vulnérabilité dans WordPress
2 novembre 2017	CERTFR-2017-AVI-387	Vulnérabilité dans Fortinet FortiClient
2 novembre 2017	CERTFR-2017-AVI-386	Vulnérabilité dans MongoDB
2 novembre 2017	CERTFR-2017-AVI-385	Multiples vulnérabilités dans les produits Apple
31 octobre 2017	CERTFR-2017-AVI-384	Multiples vulnérabilités dans le noyau Linux d'Ubuntu

VOIR TOUS LES AVIS »

Where are vulnerabilities found?

- Operating System
- Web Applications
- Database
- Business Applications
- Software and Software Packages
- Embedded Systems (planes, cars, etc.)
- Networks ...

Types of vulnerabilities

1.Software Vulnerabilities

Buffer Overflow: Writing data beyond allocated memory, leading to code execution.

Injection Flaws: SQLi, XSS, or OS command injection.

Misconfigurations: Default passwords, open ports, or exposed databases.

2. Hardware Vulnerabilities

Spectre/Meltdown: CPU flaws allowing data leaks via side-channel attacks.

Mirmware Vulnerabilities: Exploitable bugs in device firmware (e.g., routers, IoT devices).

3. Human-Centric Vulnerabilities

Weak Passwords: Easily guessable or reused credentials.

Social Engineering: Exploiting human trust (e.g., phishing).

4. Network Vulnerabilities

Unencrypted Communication: Data transmitted in plaintext (e.g., HTTP).

Outdated Protocols: Use of deprecated protocols like SSLv3 or Telnet.

Vulnerability authors

Very often by vulnerability researchers

- Professionals
  - Team from major IT security companies
  - Symantec, Kaspersky, ISS, Rapid7 …
- Cyber army
- Intelligence agencies

Vulnerabi authors

- Independent
  - Field of research on par with others
  - Source of financial revenue
  - Example
    - Hacked Google Chrome for $60,000
  - Software publishing company

Vulnerability discovery methods

- **Reverse engineering**
  - activity that involves studying an object to determine its internal workings or manufacturing method.
- **Stress test**
  - Fuzzing is a technique for testing software. The idea is to inject random data into the inputs of a program. If the program fails (for example, by crashing or generating an error), then there are defects to correct.
- Code audit
  - Direct acquisition of the code
  - Acquisition of code through decompilation
  - At this stage, use specialised tools for specific research

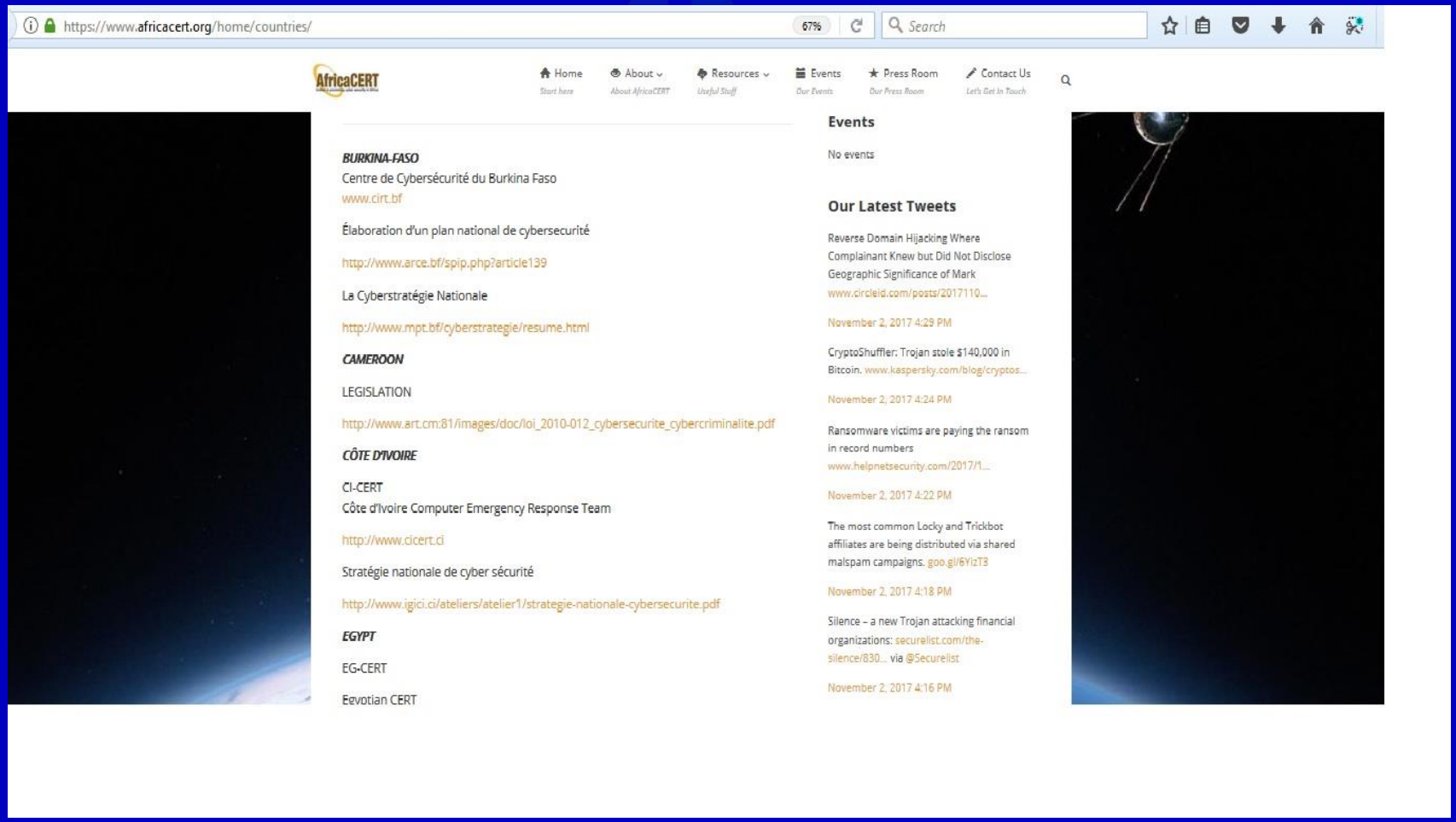
After vuln[illegible]bility discovery

- Inform the software publisher
- Inform the organisation responsible for the resource
- Inform the local CERT
- Assist with the correction
- Await the advice or security bulletin to be issued by the publisher, along with the patch if possible
- Await the thanks or financial reward

DI VERY: after a discovery?

- **Publication without a patch**
  - Publication without informing the owner of the resource
- **Publication of an exploit**
  - Programme enabling the exploitation of a vulnerability (the favourite of script kiddies)
- Exploitation by worms and malware
- E.g. Sasser, Nimda, Stuxnet …

Referencing Vulnerabilities



Referencing vulnerabilities

- QUI SOMMES-NOUS ?
- SERVICES
- DOCUMENTATION
- OUTILS DE SECURITE
- ACTUALITES

MAILING LIST DU CI-CERT

Inscrivez votre e-mail ici...

valider

INCIDENTS

- Déclarer un incident informatique
- Déclarer un cas de cyberescroquerie
- Consulter votre dossier

SURVEILLANCE SITE WEB

Entrez votre url ici...

valider

LIENS RAPIDES

- Quelques chiffres sur les attaques

Vous êtes ici : Accueil -- Avis de sécurité -- Vulnérabilités -- Détails

VULNÉRABILITÉ DANS CISCOWORKS PRIME LAN MANAGEMENT

Référence : VUL-221/MAI2012/CI-CERT , DATE : 11-05-2012

Classification de la vulnérabilité

Risque :

Atteinte à la confidentialité des données.

Information sur le(s) système(s) impacté(s)

Système(s) affecté(s) :
Versions antérieures à Cisco Prime LAN Management 4.2.

Systèmes associés :
IBM

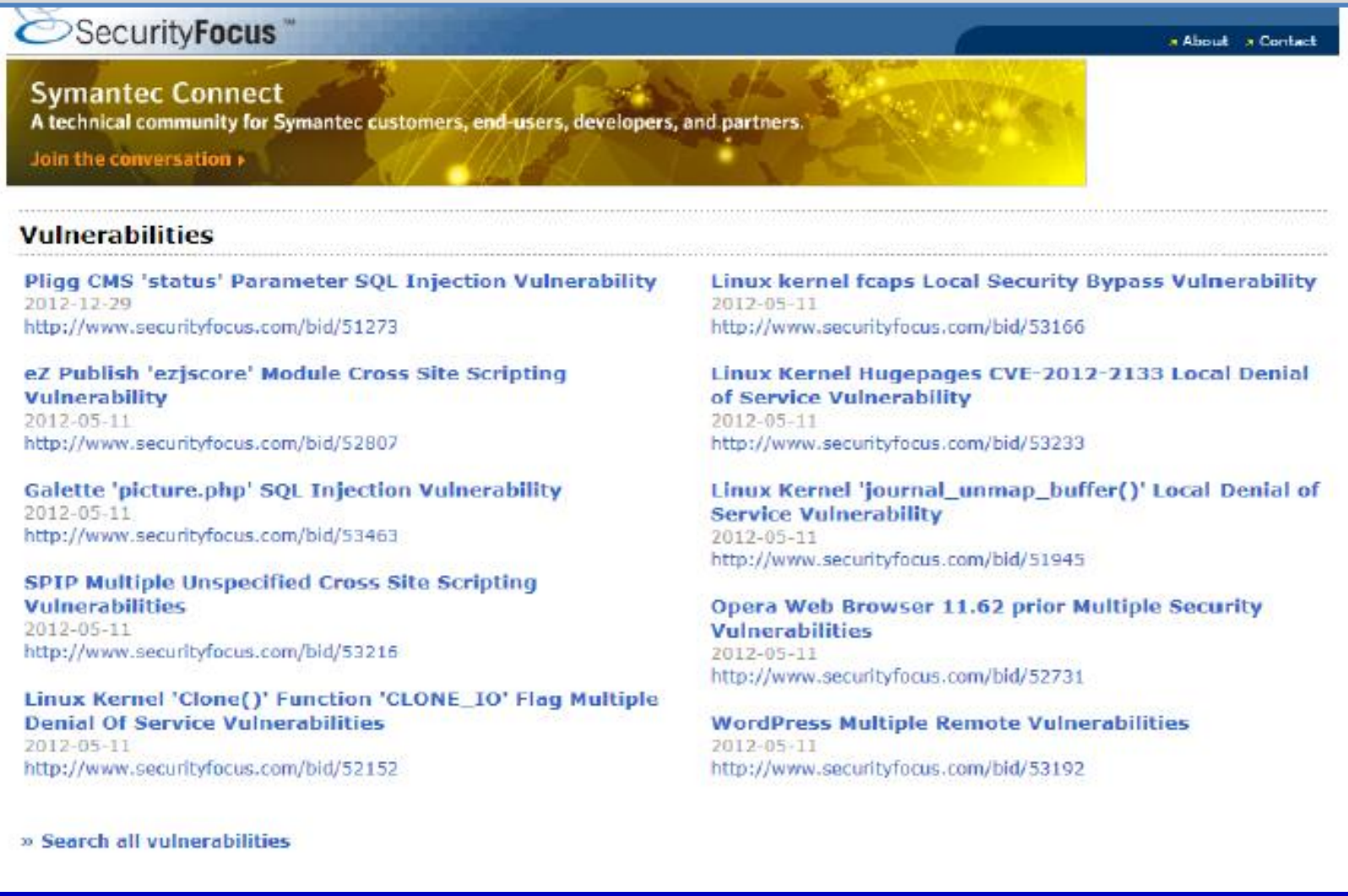
Description

Analyse détaillée :
Une vulnérabilité a été corrigée dans Cisco Prime LAN Management. Elle concerne une vulnérabilité Apache Tomcat permettant à un attaquant de falsifier des requêtes AJP et ainsi d'obtenir des informations sensibles.

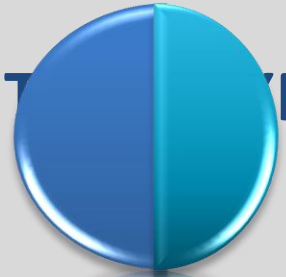
Solution

Documentation :
Bulletin de sécurité Cisco LM42REL

Referencing vulnerabilities



EVOLUTION OF EXPLOITATION

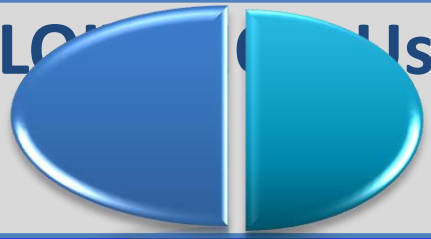


- Concept of exploit
- Example of exploit
- Useful for … !

EXPLOITATIO oncept of exploit

- An exploit is, in the field of information security, a piece of code that allows an individual or malicious software to exploit a security vulnerability in an operating system or software, either remotely (remote exploit) or on the machine where this exploit is executed (local exploit), in order to take control of a computer or network, to enable privilege escalation of software or a user, or to carry out an attack.

EXPLO[illegible] Useful for … !



- Design of worms
- Penetration testing
- State intelligence services
- Malicious individuals (cracker)
- Many others too ...

PART C SOLUTIONS

- Monitoring
- Secure design

SOLUTIONS

- **Conduct monitoring**

–Keep informed of the latest vulnerabilities

•E.g. subscribing to mailing list www.cicert.ci

http://www.certa.ssi.gouv.fr/

- Design systems and architectures that limit the impact of newly discovered vulnerabilities

The vulnerability management lifecycle

- **Vulnerability management is an ongoing process that helps organizations proactively address security weaknesses before they can be exploited. It includes the following steps:**
- **Asset Discovery** & Inventory Management
- **Discovery**: Scanning systems for vulnerabilities.
- **Prioritization**: Using CVSS scores to rank risks.
- **Remediation**: Patching, configuration changes, or workarounds.
- **Verification**: Re-testing to confirm fixes.
- **Reporting**: Documenting actions for compliance (e.g., GDPR, HIPAA).

Asset Discovery & Inventory Management

Why Asset Discovery is Critical

The Foundation: Accurate asset inventory enables effective vulnerability management.

Common Challenges:

- Shadow IT and unauthorized devices
- Cloud instances spun up without tracking
- Mobile and remote devices
- Third-party connections
- Legacy systems

Asset Discovery & Inventory Management

Objective:

Identify all assets (hardware, software, networks, and data) in the organization

Process:

- Use automated tools to discover assets
- Maintain an up-to-date IT asset inventory

Vulnerabiliti[illegible]entification

Objective: Detect various vulnerabilities in the system, network, and applications.

Methods:

- Automated analysis: Use vulnerability scanners (e.g., Nessus, Qualys, OpenVAS) to identify known vulnerabilities.
- Manual testing: Perform penetration tests or code reviews for further analysis.
- Threat intelligence: Stay informed of new vulnerabilities (e.g., CVE database, vendor advisories).

Result: A list of vulnerabilities with details such as severity, affected

Risk assessm nd prioritization

Objective: Assess the risk posed by each vulnerability and prioritize remediation efforts.

Factors to consider:

- Severity: Use Common Vulnerability Scoring System (CVSS) scores to assess severity.
- Exploitability: Is the vulnerability being actively exploited in real life?
- Asset Criticality: How important is the affected system or data to the organization?
- Business Impact: What are the potential consequences of exploitation?

Remediation

Objective: Patch or mitigate vulnerabilities to reduce risks.

Remediation Options:

- Remediation: Apply vendor-supplied security patches or updates.
- Configuration Changes: Modify system settings to reduce exposure.
- Compensating Controls: Implement temporary measures (e.g., firewalls, intrusion detection systems) until a permanent patch is available.
- Decommissioning: Remove or replace outdated or unsupported systems.

Challenges: Balancing remediation with operational continuity and resource constraints.

-

Verificat

Objective: Confirm that vulnerabilities have been successfully remediated.

Methods:

Re-analyze systems to ensure vulnerabilities are no longer present.

Validate that patches or configuration changes are applied correctly.

Result: Updated vulnerability status and proof of remediation.

Reportin

Objective: To track and communicate the effectiveness of the vulnerability management program.

Key Indicators:

- Number of vulnerabilities identified, remediated, and outstanding.
- Time to detect and remediate vulnerabilities (MTTD, MTTR).

Risk reduction over time.

- Reporting: Share results with stakeholders, including IT teams, management, and auditors.

TOP 5 common vulnerabilities

- **Missing patches:**
  - All an attacker needs is a missing patch on a server that allows unauthenticated command prompt access or another backdoor path in the web environment.
  - **Solution**
  - Install the latest security patches for the operating system and other installed applications.

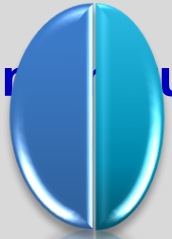
TOP 5 common vulnerabilities

- **Default or weak passwords:**
  - many web applications, content management systems, and even database servers are still configured with weak or default passwords.
  - **Solution**
    - Regularly change and test weak passwords and consider using a password management tool.
    - Implement account lockout after a defined number of unsuccessful login attempts.

TOP 5 common vulnerabilities

- **Misconfigured firewall rulebases:**
  - Searching in a rulebase of a firewall that has never been audited will inevitably lead to serious configuration weaknesses that allow unauthorised access in the web environment. Sometimes, it's direct access, while other times, it's indirect from other segments of the network, including Wi-Fi – or network segments that have been long forgotten.

TOP 5 comm[illegible]ulnerabilities



- **Mobile devices:**
  - Unencrypted phones, tablets, and laptops pose the greatest risks to web security. Consider all the VPN connections, cached passwords in web browsers, and emails containing sensitive login information that you have stored on mobile devices. Using unsecured (and rogue) Wi-Fi via mobile devices is the icing on the cake.

TOP 5 comm ulnerabilities

- **USB Flash Drives:**
- USB drives are also one of the most common ways to infect a network behind a firewall.

- Today, your computer network has a high level of security.
- But what about tomorrow? Indeed, new vulnerabilities are discovered every day.
- How can you be alerted as early as possible to the presence of a vulnerability affecting your equipment?
- This problem can be addressed through regular vulnerability audits and the adoption of a proactive approach.

Vulnerability Audit

- ***Definition***

  The vulnerability audit allows for an automated and comprehensive approach to security testing.
- It should assess the level of security and check the impermeability of the network. In cases where the results are unsatisfactory, the vulnerability audit must lead to a remediation process for the discovered vulnerabilities.

Usage

- Vulnerability scanners can be used for legal or illegal purposes:
  - **legal purposes: corporate cybersecurity experts use vulnerability scanners to find flaws in their companies' IT systems and communication systems to correct them before hackers can exploit them;**
  - **illegal purposes: hackers use the same tools to find weaknesses in corporate systems to exploit them to their advantage.**

Why conduct a technical audit?

- The technical audit informs your organisation of its potential vulnerabilities to attacks and proposes solutions to remedy them.
- A technical audit will allow you to answer, among other questions:
  - Are our confidential data protected?
  - Is it possible to gain unauthorised access to our information assets (website, corporate network, etc.)?
  - Is it possible to fraudulently order items on our e-Business site?
  - Can a customer fraudulently access another customer's account?
  - Can our websites or networks be made unavailable?
  - Can a hacker take control of one of our assets?

The quality of a vulnerability audit solution

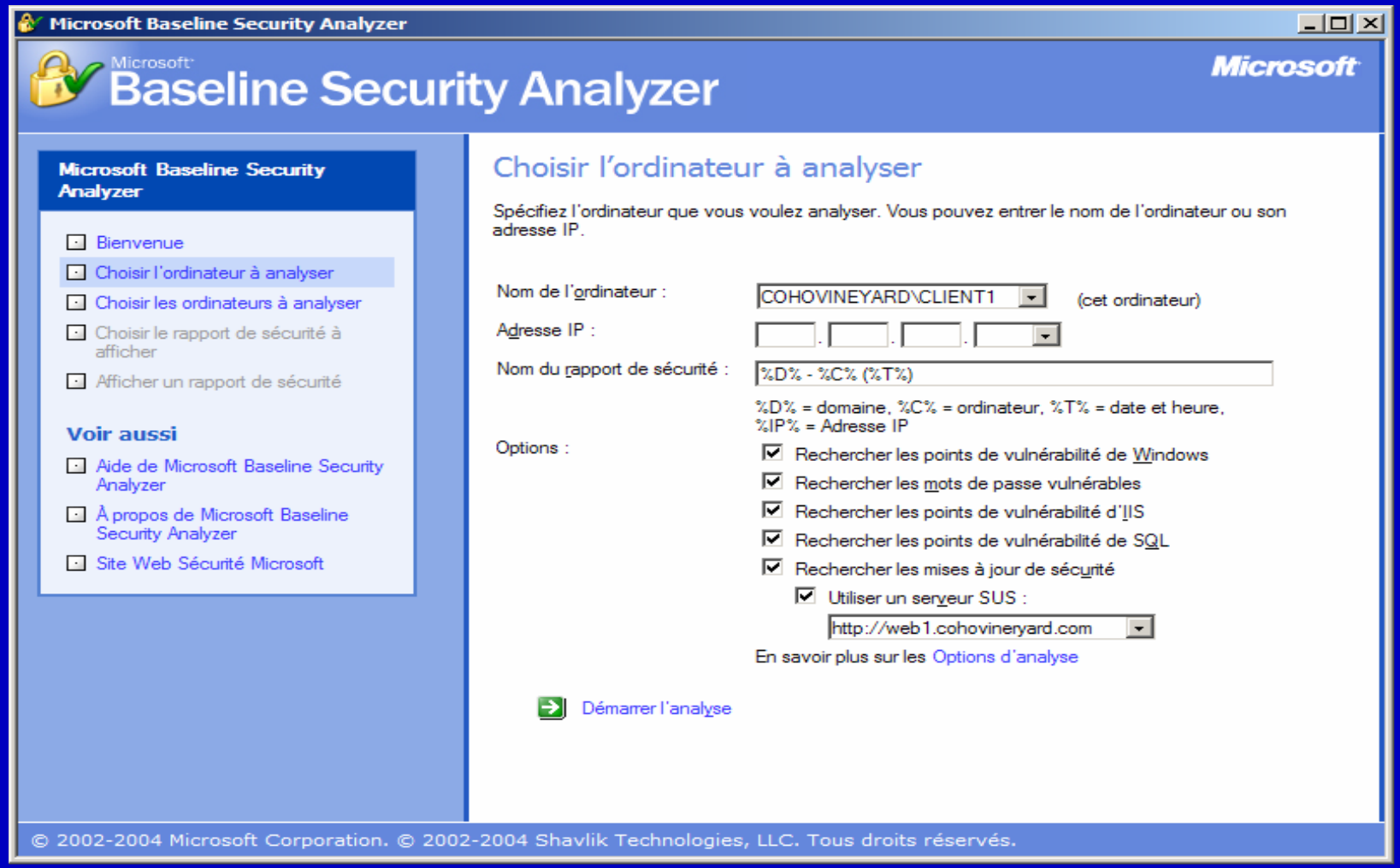
- The size and frequency of updates to the knowledge base.
- The accuracy of vulnerability detection, particularly in relation to the issues of false positives or false negatives.
- The solution's ability to extract detailed and actionable reports for technicians or IT management.
- The solution's ability to adapt to the company, especially concerning the challenges of centralising the management of the solution and multi-site business issues.

Network vulnerability tools

- ***MBSA***
- MBSA is a security vulnerability analysis tool that informs you of the status of client computers and servers. MBSA is compatible with Windows. It checks for common configuration errors in the operating system, Internet services (IIS), Microsoft SQL Server, and desktop applications, and can verify missing security updates for Windows, IIS services, SQL Server, and Microsoft Exchange Server.

Network vulnerability tools

- ***MBSA***



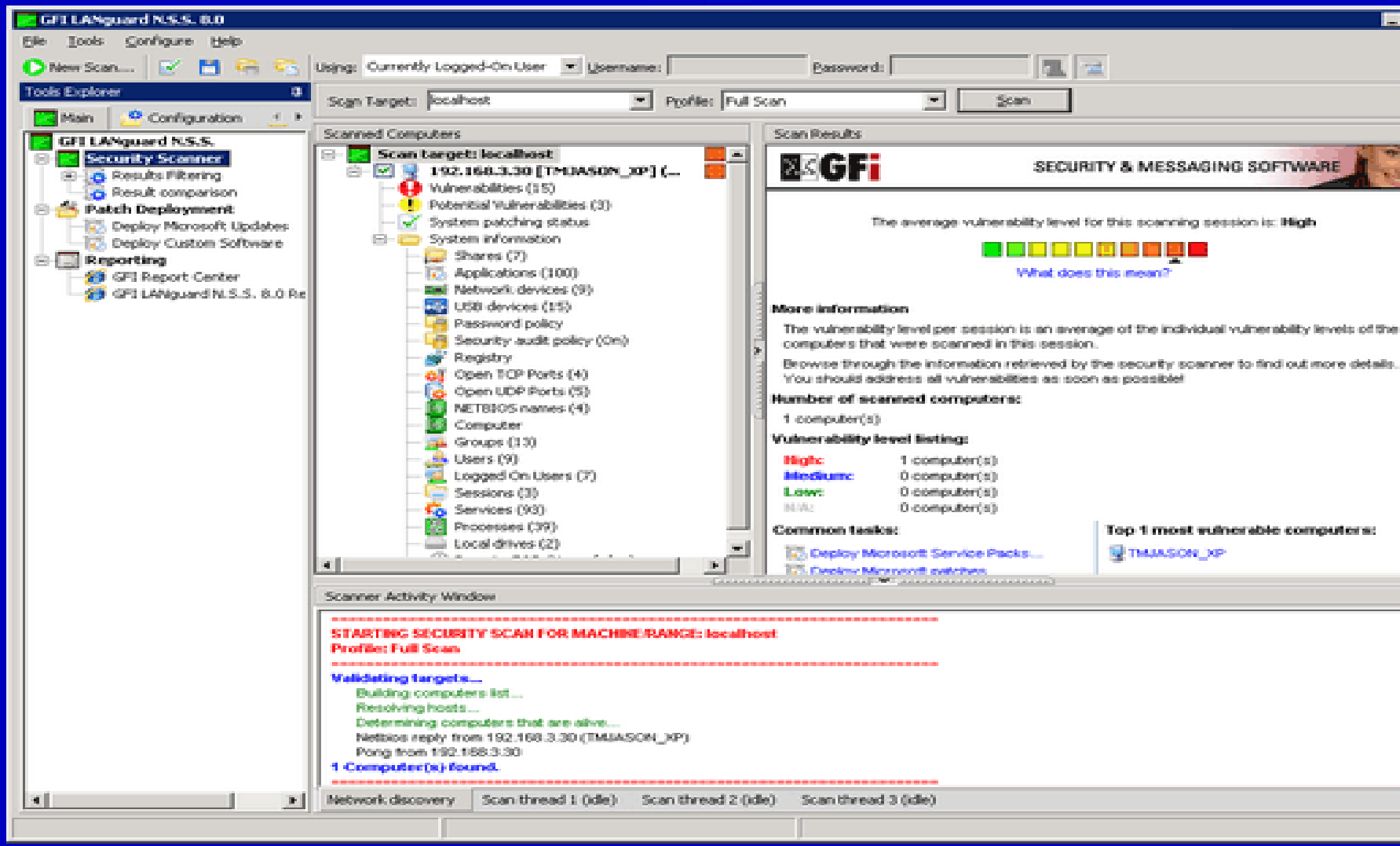
Network vulnerability tools

GFI LANguard

GFI LANguard Network Security Scanner (N.S.S.) is a solution that addresses the three pillars of vulnerability management: security scanning, patch management, and network inspection, with a single integrated console.

- By scanning the entire network, it identifies all possible security issues and
- using its powerful detailed reporting functionality,
- it gives you the tools you need to detect, assess, report, and remediate all

Network vulnerability tools



Course Questions4

- Q1: Why there are always vulnerabilities in computer systems?
- Q2: What is the role of CERT?
- Q3: Who are the authors of vulnerabilities?
- Q4: Name the methods of vulnerability discovery?
- Q5: What is an exploit?
- Q6: How can you be alerted as soon as possible to the presence of a vulnerability affecting your equipment?
- Q7: What characteristics should be considered when choosing a good vulnerability audit?