



With financial support from the Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks Programme European Commission - Directorate-General Home Affairs

The new NISHA portal

Bence Birkas, NISZ Ltd.

Overview



Why Drupal?

The workflow

Basic portal features

Access to nodes



Why Drupal?



Widely used, well supported open source content management platform

Module based

- Numerous freely accessible modules
- Easy to implement self-developed modules

Easy to customize

- Portal layout structure
- Graphic design

Each portal can use their own design or template

Easy to manage multiple language sites



Workflow



FISHA

- The portal and the network used different publication mechanisms
- In some circumstances publishing articles from the network to the portal or pushing articles from the portal to the network was uneasy

NISHA

- Reconsidered, simplified workflow
- Simplified publishing mechanism



Basic portal features



There are five different user roles that can be distinguished, which are:

Visitor roles -> view available articles in newsfeed, in details, advanced search

Guest

User -> create user profile

Maintainer roles

Operator -> create articles

Supervisor

Site Administrator





NAVIGATION

- ▼ Add content
 - Article
- Aggregated items
- Browse network
- Browse site
- Newsnotification
- Nisha profiles

Add content

Create Article

New content: *Your draft will be placed in moderation.*

Language

English ▼

English title *

Microsoft Windows Active Directory LDAP Query Handlir

This field has to be filled in English!

English short description *

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious users to cause a DoS (Denial of Service).

This field has to be filled in English!

Network?








push to network

Article type *

Advisory ▼

Save

Body (Edit summary)

B *I*    Normál              

img-left



The vulnerability is caused due to an error within the implementations of Active Directory, Active Directory Application Mode (ADAM), Active Directory Lightweight Directory Service (AD LDS), and Active Directory Services when handling LDAP queries. This can be exploited to exhaust available memory resources and render the LDAP service non-responsive via a specially crafted LDAP query.

body p img

Text format **CKEditor**

[More information about text formats](#)

Allowed HTML tags: `<a>` `` `` `<blockquote>` `` `` `` `<h2>` `<h3>` `<h4>` `<h5>` `<h6>` `<p>` `<pre>` ``

Insert image

File information	Operations
   hacker 5_12.jpg (6 KB)	Remove
Style: medium	Insert

Add a new file

[Browse...](#) [Upload](#)

Files must be less than 2 MB.

Allowed file types: **png gif jpg jpeg**.

Characterize the content ▾

Network?

push to network

Check if the article will be pushed into the network

Keywords *

sérülékenység, IBM

Add tags for the article in the language of publicaton. Tag is a non-hierarchical keyword or term assigned to a piece of information. This metadata helps to describe an item and allows it to be searched by browsing. Each keyword has to be separated by comma (example: Social network, security, data theft,...)

English keywords *

vulnerability, IBM

Add keywords for the article in English. Keyword is a metadata that refers to the content of the publicaton. Each keyword has to be separated by comma (example: Social network, security, data theft,...)

RESOURCE

	Title	URL
+	IBM Tivoli Endpoint Manager LDAP	http://secunia.com/advisories/552

The link title is limited to 128 characters maximum.

Add external links related to the article or other contents which were the basis of the article.

Add another item

Profiles

--Select-- ▾

Categories ▾

Threat level *

- None
- Low
- Medium
- High

Choose the risk classification of the article. This marks how seriously the threat affects the users; if there is an exploit publicly available for a vulnerability; if anti-virus softwares recognize the malware; if the threat affects widely used application, etc.

Target groups *

- Adults
- Kids
- Silver Surfers
- Teenagers

Choose the social groups who the article is addressed to.

Categories

- News
- Awareness Raising
- Mobile
- Android
- iOS
- Social networking
- Facebook
- Twitter
- Google+
- Hardware
- Security
- Software

Attachments

Add a new file

Tallózás... Nincs kijelölve fájl.

Upload

Files must be less than **10 MB**.

Allowed file types: **txt doc docx xls xlsx ppt ppts pdf jpg png**.

Extended Info

Add detailed vulnerability and CVE information related to the article.

Damage Description

spoofing attacks

Add description of the damage caused via exploiting the vulnerability.

Vulnerability Description

authentication error

Add detailed information about the vulnerability.

Consequences Description

Possible Solution

Update to version 9.0.787 (patch 4).

Add existing solution and mitigation methods related to the vulnerability.

Further features



Publish existing portal content to the network

Translate portal content on the portal

Browse Network

Publishing existing article from the network

Translating single article from the network

Creating new article based on multiple network entities

Creating new article from aggregated items

News notifications



Access to nodes



Halozatbiztonsag.hu

nisha.cert.pl

nisha2.cert.pt

nisha2.if-is.net

Project website: nisha-network.eu



Lessons learned

Overview



Operational issues

Cooperation experience

Organizational aspect

Legal considerations



Operational issues



General awareness or more more technical?

Amount of articles in the network does not reach the critical mass

Due to low promotion, no registered users with profiles to give hints on interested content

No fixed direction on type of information

Much of the information is duplicated from other primary sources

Further developments and improvements are in concept phase



Cooperation experience



Need to find the right community to operate the network

Local workshops prove interest in local portals

The potential of sharing via networking is not exploited: experiments carried out to prove the concept and test network functionalities

SNS beat the concept of information brokers



Organizational aspects



Funding: if concept/infrastructure is viable, long term and sustainable funding is needed on SLA basis

Governance: roles and responsibilities are needed to define at network level management

Metrics are needed to support the viability of the network

