

[NEWS] eNom Domain Registration Services Domain Hijacking Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0021.html>

From: support@securiteam.com

Date: 02/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 4 Feb 2002 20:15:19 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

eNom Domain Registration Services Domain Hijacking Vulnerability

SUMMARY

<<http://www.enom.com>> eNom provides Internet domain name services. A security vulnerability in the way they handle email-based confirmations allows attackers that gain access to bounced email to hijack domain names stored under eNom.

DETAILS

When you become a member of eNom, you get a user name and a password. With this password and user name you can register domains, transfer domains, change contact information from the panel. You have two choices when transferring domains with eNom.

First, one is authorization with Fax. With fax, the owner of the domain sends the needed information of the new domain owner, and the transferring begins.

The second one is the electronic authorization. The transferring begins with the e-mail sent to the domain owner e-mail on the contact information. In this mail, there is a web address for approval or refusal. When you enter this site, you may start the transferring with either

Securiteam: [NEWS] eNom Domain Registration Services Domain Hijacking Vulnerability

pressing the "approve" or "reject" button. In the mail below <hostmaster@acme.xxx> mail address is eNom members' mail, it is the mail address given by the owner of the panel when becoming a member of eNom. The mail sent to the contact person whose domain will be transferred is sent through this mail address, and persons' or firms title is written. The mail address is <hostmaster@acme.xxx> in the below mail. In addition, the owner of the panel title is <Acme Inc.>. Moreover, the owner of the domain owner's mail is <domaincontact@example.xxx>. The mail below is the mail sent after the order of transferring.

-----SNIP-----
From: Acme Inc. <hostmaster@acme.xxx>
To: <domaincontact@example.xxx>
Subject: Domain Transfer Request for EXAMPLE.XXX

Dear Customer,

You are receiving this notice because your are listed as one of the contacts for the domain name EXAMPLE.XXX.

We have received a request to transfer this domain name to a new registrar, Acme Inc. Please click on the following URL link and let us know if you approve OR disapprove this domain transfer:

PLEASE NOTE: if the link below is broken you will need to copy and paste everything between < > into your browser

<<http://www.transfer-approval.com/universal.asp?id=A000000-7D0A-0F60-9000-14005050B010>>

The deadline for responding to this request is: Jan 06, 2002.

Thank you for your time and attention regarding this matter. If you have any questions please reply to this e-mail.

Sincerely,
Acme Inc.

-----SNIP-----

Exploitation:

When the domains owner receives the above mail and then whenever he approves it, "almost like every domain resellers" without any "approval" the domain is transferred to the new owner. In this case, let us think the domain's mail address is non-functioning. If the domain contact mail is closed, the sent mail is returned from the mail server. This is where the problem begins. The mail sent to the domains contact mail from eNom's, the person who likes to transfer the domains mail is sent through <hostmaster@acme.xxx> but because of it's sent by eNom and if the mail is closed it returns back to <hostmaster@acme.xxx> and in this mail you can find the URL sent for refusal or the approval. The person can follow the URL and approve this transfer and the required domain will be transferred to eNom. Below you can find an example returned mail.

Securiteam: [NEWS] eNom Domain Registration Services Domain Hijacking Vulnerability

-----SNIP-----
From: <MAILER-DAEMON@mail.acme.xxx>
To: <hostmaster@acme.xxx>

Hi. This is the qmail-send program at mail.acme.xxx. I'm afraid I wasn't able to deliver your message to the following addresses. This is a permanent error; I've given up. Sorry it didn't work out.

<domaincontact@example.xxx>:
209.228.xx.xx does not like recipient.
Remote host said: 550 User unknown
Giving up on 209.228.xx.xx.

- - - - Below this line is a copy of the message.

Return-Path: <hostmaster@acme.xxx>
--0000
Received: from unknown (HELO acme)
(hostmaster@acme.xxx@[217.131.xx.xx]) (envelope-sender
<hostmaster@acme.xxx>
by 195.244.xx.xx (qmail-ldap-1.03) with SMTP
for <domaincontact@example.xxx>; 20 Jan 2002 11:16:56 -0000
Message-ID: <001701c1a1a4\$1c209390\$0b8883d9@acme>
Reply-To: "Acme Inc." <hostmaster@acme.xxx>
From: "Acme Inc." <hostmaster@acme.xxx>
To: <domaincontact@example.xxx>
Subject: Domain Transfer Request for EXAMPLE.XXX
Date: Sun, 20 Jan 2002 13:17:55 +0200
Organization: <http://www.acme.xxx>
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000

Dear Customer,

You are receiving this notice because you are listed as one of the contacts for the domain name EXAMPLE.XXX.

We have received a request to transfer this domain name to a new registrar, Acme Inc. Please click on the following URL link and let us know if you approve OR disapprove this domain transfer:

PLEASE NOTE: if the link below is broken you will need to copy and paste everything between < > into your browser

<<http://www.transfer-approval.com/universal.asp?id=A000000-7D0A-0F60-9000-14005050B010>>

Securiteam: [NEWS] eNom Domain Registration Services Domain Hijacking Vulnerability

The deadline for responding to this request is: Jan 06, 2002.

Thank you for your time and attention regarding this matter. If you have any questions please reply to this e-mail.

Sincerely,
Acme Inc.

=====SNIP=====

Conclusion:

As we have explained above, any contact mail that is no longer receiving emails (i.e. closed), can have its domains transferred through eNom.

Solution:

eNom fixed this issue January 21, 2002.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ts@securityoffice.net> Tamer Sahin.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NEWS] Intel WLAN Driver Stores 128bit WEP-Key in Plain Text"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)