

Re: Citrix exploits?

## Re: Citrix exploits?

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-08/msg00334.html>

---

- *From:* "r@d" <m2rad@xxxxxxx>
  - *Date:* Fri, 18 Aug 2006 22:54:38 +0200
- 

This is quite hard to do, because Citrix Web Interface, usually is installed in conjunction with Citrix Access Gateway or Citrix Secure Gateway, that inherits a ticketing system to validate the requested session. If you could break the Citrix Web Interface by exploiting one of the .dll's its using, or finding error's in the .cs or .js files included with Web Interface (serverside/clientside folder) it would be possible to get unauthorized access to the application list, once there, it should be no problem requesting a ticket for a session. Citrix has several security bulletins on their website (support.citrix.com) how this is done with two factor 'protected' sites, where if two factor fails, a path to the applist.htm is available to get unauthorized access to the application list. Still you would need a username/password (ie test/test) to initially authenticatie. A more easy option: Usually Citrix Web Interface is installed as local administrator on IIS, break IIS, and you break Web Interface.

regards, Rajendra Soebhag

----- Original Message ----- From: "Marc Ouwerkerk" <marc@xxxxxxxxxxxxxxxx>  
To: "Ben Nell" <enemy.cow@xxxxxxxx>; <pen-test@xxxxxxxxxxxxxxxx>  
Sent: Monday, August 14, 2006 5:12 PM  
Subject: RE: Citrix exploits?

If you have a valid user name and login, you can check if one of the MS applications installed (Word, Access, etc) have VBA enabled. You can then execute any dll that you upload to the machine.

Marc Ouwerkerk

-----Original Message-----  
From: Ben Nell [<mailto:enemy.cow@xxxxxxxx>]  
Sent: maandag 14 augustus 2006 5:56  
To: pen-test@xxxxxxxxxxxxxxxx  
Subject: Re: Citrix exploits?

On 11 Aug 2006 22:35:38 -0000, 09Sparky@xxxxxxxx <09Sparky@xxxxxxxx> wrote:

Does anyone have any good techniques or exploits available for Citrix

(web)? I am working on exploiting a citrix server with a front end webpage, but am unsuccessful. Any suggestions/thoughts?

Re: Citrix exploits?

Re: Citrix exploits?

Do you have a valid user name and login for the Citrix farm? If the launch.ica files (provided as links, once logged into the web interface) can be downloaded and opened in a text editor, they will provide you with information about the connection that the farm is set up to use. Is the web interface using SSL? If the site's running over SSL, it's possible that they have their farm behind a Citrix Access Gateway (AG) or MetaFrame Secure Access Manager (MSAM). In the case that an AG or MSAM is deployed, the connection is encrypted on the backend, otherwise you should be able to capture session information on the backend. You can tell if one of these technologies is in use because ports 1494 (ICA) and 2598 (session reliability) will not be open in such a setup.

I would also note the type of farm that's set up. Citrix "best practice" suggests setting up a farm using the naming convention "meta01" for the first server in the farm and moving up. I would check for additional DNS names using the same convention.

---

---  
--  
This List Sponsored by: Cenzic

Concerned about Web Application Security?  
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php)  
And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxxx for details.

---

---  
--  
This List Sponsored by: Cenzic

Concerned about Web Application Security?  
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php)  
And, now for a limited time we can do a FREE audit for you to confirm your

Re: Citrix exploits?

results from other product. Contact us at request@xxxxxxxxxx for details.

---

---

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

[http://www.cenzic.com/products\\_services/download\\_hailstorm.php](http://www.cenzic.com/products_services/download_hailstorm.php)

---