

[Full-disclosure] Oday: Hacking secured CITRIX from outside

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-10/msg00241.html>

- *From:* "pdp (architect)" <pdp.gnucitizen@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 10 Oct 2007 16:47:23 +0100
-

<http://www.gnucitizen.org/blog/Oday-hacking-secured-citrix-from-outside>

In the true spirit of GNUCITIZEN half(partial)-disclosure initiative, we announce that it is possible to gain user access level on integrated remote CITRIX servers. The bug/feature does not relay on any client/server vulnerabilities nor client/server misconfiguration issues. All an attacker needs to do to exploit the weakness is to lure a victim, part of an integrated network, to a malicious website or trick them into opening specially crafted ICA files. The attack results into remote command execution with the access level of the current user.

The success of the attack relays on the fact that the victim (the proxy) is part of a CITRIX ring to which he/she can perform pass through authentication. Once a connection is instantiated, the victim will unwillingly and transparently login into CITIRIX and perform several commands specified by the attacker. The attacker can simply instruct the remote desktop to download files from a remote TFTP server and execute them locally. Once the attack is performed, the local connection is terminated and the CITRIX session is cleared. No user interaction is required!

CAUTION!!! The attack can be used to circumvent/bypass border firewalls and sneak into private networks. This attack is of type CRSF (Cross-site Request forgery), although it does not relay on Web bugs. The attack vector works flawlessly on IE and Firefox (when configured correctly). It also works with any email client or other types of file sharing mechanisms. All versions of CITRIX and CITRIX client are affected. The attack may fail on certain setups.

If you manage to re-discover the type of vulnerability outlined in this post, we encourage you to keep it private. Give some time for the folks at CITRIX to react. Currently, I am not aware of any remedy against the attack. Given CITRIX's popularity among corporations and big organizations, it is highly recommended to take this warning with extra caution.

[Full-disclosure] Oday: Hacking secured CITRIX from outside

pdp (architect) | petko d. petkov

<http://www.gnucitizen.org>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>