

# [NT] Blaxxun3D Romote Buffer Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0018.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 04/07/04

To: list@securiteam.com

Date: 7 Apr 2004 16:45:10 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Blaxxun3D Romote Buffer Overflow

---

## SUMMARY

<<http://www.blaxxun.com>> blaxxun3D offers "an easy and cost-effective way to for businesses and organizations to develop, deploy and maintain collaborative virtual environments for web community and conferencing applications".

The program registers a custom file type allowing an attacker to overflow the URL property used by the object and cause the program to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* blaxxun3D platform version 7

Blaxxun Platform 7 registers the following application type: "application/x-cc3d". After the first time the platform was used, this type of object can be created locally and remotely (using a browser).

The vulnerability resides in the "URL" property of the object. Sending it a long argument will cause the program to overflow an internal buffer that in turn causes the program to execute arbitrary code.







Securiteam: [NT] Blaxxun3D Remote Buffer Overflow

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