

Mysterious "Support" account created on Win2k server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-01/0022.html>

From: Ostfeld, Thomas (tostfeld@kimpact.com)

Date: 01/02/03

From: "Ostfeld, Thomas" <tostfeld@kimpact.com>

To: "'incidents@securityfocus.com'" <incidents@securityfocus.com>

Date: Thu, 2 Jan 2003 15:33:54 -0500

One of my web servers appears to have had an intrusion. The box is Win2k Advanced Server, SP3, up to date on all security patches. I first became aware of a problem when the main website hosted on the box became inaccessible. Checking the machine, I discovered that the Local Security Policy had been altered as to remove the Everyone and Local Administrators group from "Access this machine from the network" policy. In place was a single local account called "Support" that I did not recognize.

Looking into the accounts database, I discovered this account with a description of "Built in account for providing user support." It was also part of the administrators group. Needless to say, this looked suspicious, so I locked the server back down and set up intrusion detection to look for further attempts to exploit the account.

I know approximately when the attack occurred, but I am still puzzled as to how it was done. The web logs show the usual IIS root exploit attempts, but those all fail. Everything else looks normal. I've scoured the machine pretty thoroughly for bots, trojans, viruses, hidden and altered files, and have so far come up empty. No weird open ports either.

Has anyone seen this before? There is one or two postings of the same nature on Google, but little else to give me something to go on.

Tom Ostfeld
Knowledge Impact
Ostfeld7 (AIM)

This list is provided by the SecurityFocus ARIS analyzer service. For more information on this free incident handling, management and tracking system please see: <http://aris.securityfocus.com>