IBM Fixes Flaw in Tivoli Provisioning Manager

April 4 2007

Remote exploitation could allow attackers to crash the service or execute malicious code with SYSTEM privileges.

IBM has patched multiple flaws in its Tivoli Provisioning Manager for OS Deployment that allowed attackers to crash the service or execute arbitrary code with SYSTEM priviledges.

Tivoli Provisioning Manager for OS Deployment is a network boot server that facilitates central management of networked workstations, implements PXE (Pre-boot Execution Environment) as well as a Web-based administration service.

The vulnerabilities exist in the handling of multi-part/form-data HTTP POST requests, according to an advisory by Sterling, Va.-based iDefense Labs. Malformed requests can cause invalid memory accesses, leading to denial of service or possibly heap corruption.

"No authentication is required to access the vulnerable code," according to the iDefense Labs advisory. "The attacker need only be able to send a specially crafted request to the HTTP (8080) or HTTP-SSL (443) port of the management service. It should be noted that this service can be run with reduced privileges. iDefense recommends running this service with the least amount of privileges possible."

IBM has addressed these vulnerabilities within Tivoli Provisioning Manager for OS Deployment 5.1 Fix Pack 2. The vulnerabilities are known to exist within version 5.1.0.116 of Tivoli Provisioning Manager for OS Deployment, and older versions may be affected as well. Employing firewalls to limit access to the affected service will mitigate exposure to these vulnerabilities, iDefense stated in the advisory.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: IBM Fixes Flaw in Tivoli Provisioning Manager (2007, April 4) retrieved 25 April 2024 from https://phys.org/news/2007-04-ibm-flaw-tivoli-provisioning.html