IBM Plugs Two Holes in Lotus Domino Security

March 29 2007

The company patches flaws that could have allowed hackers to execute code remotely in Lotus Domino Web Access, Lotus Domino Server 7.0.1

IBM has patched two vulnerabilities uncovered last year in its Lotus Domino product line.

Both vulnerabilities were fixed in Lotus Domino 6.5.6 and 7.0.2 Fix Pack 1. Last August, Sterling, Va.-based iDefense Labs reported a cross-site scripting vulnerability affecting IBM Lotus Domino Web Access, a Web-based messaging and collaboration interface for the Lotus Domino server.

"The vulnerability specifically exists due to improper HTML filtering of e-mail message contents. Although Web Access attempts to filter out HTML and script code, certain code sequences will bypass the filters and successfully execute JavaScript," according to iDefense.

IBM officials stated in an advisory that the Active Content Filter feature needed to be updated to thwart the attack.

The second flaw is a heap overflow vulnerability affecting IBM Lotus Domino Server software, which provides messaging and scheduling capabilities on a number of operating systems. If a hacker were to exploit the vulnerability in the directory service (LDAP) component of IBM's Lotus Domino Server 7.0.1 remotely, the hacker could cause a denial of service or execute arbitrary code. It was reported to IBM by iDefense in October.

"When a malformed request is made to the LDAP component of a Lotus Domino Enterprise Server, a heap overflow can be triggered," according to a security alert posted by iDefense. "The vulnerability specifically exists in the handling of strings larger than 65,535 bytes. When a string longer than this value is encountered, the service allocates memory using only the lower 16 bits of the string length. Since the entire string is subsequently copied into the newly allocated buffer, a heap-overflow occurs."

Although the service does not run as root, it does run as the same user as many other components of the Lotus Domino Server and therefore an attacker may gain access to sensitive information or subvert the server. In order to attempt exploitation, however, attackers must be able to connect to the LDAP service, according to the iDefense advisory.

Citation: IBM Plugs Two Holes in Lotus Domino Security (2007, March 29) retrieved 23 April 2024 from https://phys.org/news/2007-03-ibm-holes-lotus-domino.html