

[NEWS] IBM Informix Dynamic Server Authentication Password Stack Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00047.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 16 Mar 2008 12:51:39 +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>

IBM Informix Dynamic Server Authentication Password Stack Overflow Vulnerability

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on systems with vulnerable installations of IBM's Informix Dynamic Server. User interaction is not required to exploit this vulnerability. Authentication is not required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

- * IBM Informix Dynamic Server

The specific flaw exists in the oninit.exe process that listens by default on TCP port 1526. During authentication, the process does not validate the length of the supplied user password. An attacker can provide a overly long password and overflow a stack based buffer resulting in arbitrary code execution.

[NEWS] IBM Informix Dynamic Server Authentication Password Stack Overflow Vulnerability

Vendor Response:

IBM has issued an update to correct this vulnerability. More details can be found at:

- <<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55210>>
- <http://www-1.ibm.com/support/docview.wss?uid=swg1IC55210>
- <<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55209>>
- <http://www-1.ibm.com/support/docview.wss?uid=swg1IC55209>

Disclosure Timeline:

- 2007-11-07 – Vulnerability reported to vendor
- 2008-03-13 – Coordinated public release of advisory

CVE Information:

- <<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0727>>
- CVE-2008-0727

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>
 The Zero Day Initiative (ZDI).
 The original article can be found at:
 <<http://www.zerodayinitiative.com/advisories/ZDI-08-012>>
<http://www.zerodayinitiative.com/advisories/ZDI-08-012>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
 To unsubscribe from the list, send mail with an empty subject line and body to:
 list-unsubscribe@xxxxxxxxxxxxxxxxx
 In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
 In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.