



Security Bulletin: For safer IBM Notes single sign on with Windows, use Notes Shared Login or Notes Federated Login (CVE-2013-0522)

Flash (Alert)

Abstract

Notes Client Single Logon uses an operating system communication mechanism for password transmission between Windows and Notes that can be attacked by malicious code planted on the user workstation to reveal the user password. To prevent the potential for attack, disable Notes Client Single Logon and instead opt to use the more secure Notes Shared Login or Notes Federated Login.

Content

CVE ID: CVE-2013-0522

DESCRIPTION

When adopting any single sign on solution, administrators face the tough trade-off between usability (a single password granting access to multiple systems) and better security (different passwords for different systems). A single password for multiple systems is obviously popular with users, while different passwords for different systems is popular with security-minded administrators. However, when these administrators prevail, users often resort to writing down multiple passwords. And so grows the demand for better single sign on solutions.

Notes Client Single Logon uses an operating system communication mechanism for password transmission between Windows and Notes that can be attacked by malicious code planted on the user workstation to reveal the password of an authenticated user. To prevent the potential for attack, disable Notes Client Single Logon and instead opt to use the more secure Notes Shared Login or Notes Federated Login.

For more information on Notes Shared Login, see

- [Using Notes Shared Login to suppress password prompts](#)

For more information on Notes Federated Login, see section "Using Security Assertion Markup Language (SAML) to configure federated-identity authentication" in

- [IBM Domino 9.0 Administrator Help](#)

For more information on disabling Notes Client Single Logon, refer to the **Note** in the following Help topic:

- [Using Notes client single logon to synchronize Notes and OS passwords](#)

For a comparison of Notes Client Single Logon and Notes Shared Login, see [technote 1437726](#).

CVSS:

Using the Common Vulnerability Scoring System (CVSS) v2, the security rating for this issue is:

CVSS Base Score: 4.1

CVSS Temporal Score: See <http://xforce.iss.net/xforce/xfdb/82531> for the current score.

CVSS Environmental Score: Undefined

CVSS String: (AV:L/AC:M/Au:S/C:P/I:P/A:P)

Access Vector: Local Access Complexity: Medium

Authentication: Single Confidentiality Impact: Partial

Integrity Impact: Partial Availability Impact: Partial

AFFECTED PLATFORMS

Any version of IBM Notes running on Windows with Notes Client Single Logon enabled.

REMEDIATION:

Workaround:

To prevent the potential for attack, disable Notes Client Single Logon and instead opt to use the more secure Notes Shared Login or Notes Federated Login.

Mitigation(s):

1. For your Notes Execution Control list settings for -Default- and -No Signature-, do NOT allow access to File system, External code or External programs.
2. Frequently change your Windows password with length and complexity commensurate to the information it protects.
3. Use Windows screen saver password to prevent unauthorized access to your workstation.

References:

[Complete CVSS Guide](#)

[On-line Calculator V2](#)

[CVE-2013-0522](#)

X-Force Vulnerability Database: <http://xforce.iss.net/xforce/xfdb/82531>

Related Information:

[IBM Product Security Incident Response Program](#)

ACKNOWLEDGEMENT

This vulnerability was reported to IBM by Markus Piéton of it.sec GmbH & Co. KG.

Change History:

24 April 2013	Initial publish
---------------	-----------------

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Flash.

Note: According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.

Cross reference information

Segment	Product	Component	Platform	Version	Edition
Messaging Applications	Lotus End of Support Products	Lotus Notes		7.0, 6.5	

Copyright and trademark information

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
