

LOTUS NOTES AND DOMINO WEB SERVER APPLICATION SECURITY RISKS AND REMEDIATION

Erik Hoover and Charles Hamilton
InfoScreen, Inc.
Ithaca, New York
www.infoscreen.com

ABSTRACT

Lotus Notes and Domino Web Server provide a powerful framework for rapidly developing and deploying business applications. While the Lotus platform has a well deserved reputation for security, this reputation often creates a false sense of protection. Security vulnerabilities abound in many publicly deployed Lotus and Domino business applications. These vulnerabilities can be easily exploited by a skilled external or internal adversary determined to uncover confidential information. Careful attention to the development and architecture of business applications combined with configurations optimized for effective security, and a program of non-automated security testing will significantly reduce the risk of unintended loss of confidential business data. This paper enumerates common security risks in the Lotus Domino application environment and details specific technical methods and business procedures to address identified concerns.

CONCENTRATED BUSINESS INFORMATION

The companies that rely on the Lotus Domino environment tend to concentrate a wealth of confidential information in the system. Financial documents are stored in intranet portals, credit card and transaction information is transmitted over eCommerce applications, and the email of the CFO is often accessed over the web. While the install base of Lotus Domino applications on the public internet is low in comparison to Microsoft and Oracle products, the wealth of information trusted to the systems by businesses that do use the products make the system an inviting target for skilled external hackers.

There is an active underground community that lists common penetration methods used to compromise Lotus Domino applications. Because of the relatively small number of businesses using this environment, hackers specializing in attacking these systems do not rely on automated scanning software to search for common vulnerabilities across thousands of companies. Rather, skilled attackers target a single company and then conduct an in-depth manual probing of applications to discover vulnerabilities. These individualized probes generally pass undetected by web applications built by necessity to allow some degree of access over the internet to anonymous users.

THE LOTUS NOTES SECURITY ENVIRONMENT

The security architecture of the Lotus Notes environment is at its core very robust. The system has been in constant development and improvement since 1989 and incorporates security functionality to meet requirements of government intelligence customers including the Central Intelligence Agency.

The primary strength of the underlying architecture of Lotus and Domino is based on the following two principles:

- 1) Ability to lock down all documents at a very fine grained level
- 2) Robust user authentication control

These controls and others, as detailed in the published Domino Security Model, allow organizations following published guidelines and working in a controlled environment to lock down data without fear of unintended release. Unfortunately business application development and IT functions are not completely controlled environments. Business requirements and feature sets change rapidly, development teams and network staff communicate with varying degrees of success, hacking tools become more sophisticated, and new software versions are constantly appearing.

SECURITY RISKS

Despite the robust nature of the underlying Domino Security Model, applications built and deployed in real-world business settings often have vulnerabilities. These vulnerabilities are commonly derived from the following security risk categories:

Rapid Application Development

One of the key selling points of the Lotus and Domino Server environments is the ability for developers to quickly build programs using Rapid Application Development tools. These tools allow an application to be quickly rolled out using a series of pre-built or slightly modified application templates. This paradigm of software development puts convenience and speed before security concerns. It has inherent security risks because it encourages developers to build an application without fully understanding all of the built in functionality and code of the original template.

To illustrate this type of security vulnerability, a hypothetical template for a simple form submission page to collect customer comments could be built quickly from a more complex template for online survey functionality. The original survey template could include code to display a running tally of other user opinions pulled from existing documents in the Lotus database. The developer building the simple form may not fully understand or remove the more complex functionality from the survey template code. Malicious users could then access this hidden code by manipulating the application query string on the new page to access possibly restricted data.

Specialized Commands

Domino has a set of specialized commands that modify presentation of data to a web browser. These commands can be found in product documentation, at the Lotus website, and in a number of online forums. These commands can be inserted into the URL string in the address bar of a web browser to reveal and access views and documents. For example, the following command typed into the URL string of an application generates XML output detailing the paths and UNIDs for the database documents:

http://systemname/databasename.nsf?readentries

These and other commands do not necessarily provide access to restricted information. An application that uses obscurity of view names to hide information – a common shortcut - will be vulnerable to plunder. Adherence to the Domino Security Model provides reliable security against these techniques. These commands and others are often the first steps an adversary will use to evaluate an application for exploitation.

Controlling Paths Does Not Control Access

Application developers in a web environment often believe that visible paths – links – are the only way for users of the application to travel to a given resource. A request for user authentication can be compared to a gatehouse on a bridge. The developer puts the gate in place and concludes that the resource on the island behind the bridge is now secure. This approach does not restrict the resource itself.

Skilled adversaries develop and popularize methods to circumvent these incomplete access controls. Misunderstanding of the Domino security model has created applications with flawed execution and has placed data of the most sensitive nature in jeopardy.

A False Perception of Security

Lotus Domino is supported and developed by one of the largest technology companies in the world and is in use in fields where security is hyper-critical. It ships with powerful but easily configured tools for authentication encryption and transaction logging. The trusted names of Lotus and IBM along with easy to access security functionality endows Lotus environments with a potentially false aura of security. Out of the box the systems do have known vulnerabilities and like other products they need to

be locked down prior to public use. Relying on the reputation of IBM, operators of the system often develop a set and forget mentality with Lotus products believing that the system will stay secure over time. This attitude coupled with the cost of software upgrades lead to many systems running on out of date versions of Lotus software with known security flaws.

REDUCING SECURITY RISK

The categories that follow can guide an organization to mitigate risk in the Lotus Domino application environment.

Avoid Common Mistakes

At a minimum - the following simple steps will take care of many common problems, these steps can be carried out with minimal effort or loss of function in most applications.

1. Patch or upgrade to 5.0.12 or 6.0 or above. Test the upgrade on a development server to identify possible conflicts before making changes on a production server. This won't save you from poor application design, but there are some serious flaws in older releases.
2. Remove development databases and other unused functionality. Remove user identities that are no longer valid.
3. At a minimum, the ACL for names.nsf, catalog.nsf, events4.nsf, bookmark.nsf, log.nsf, webadmin.nsf, and domlog.nsf should be set to No Access for Default and Anonymous. This is good practice for all Domino servers. During this process lock down the associated templates as well.
4. Use the action Upgrade To More Secure Internet Password Format and set the Directory Profile option Use More Secure Internet Passwords. Both features are described in Domino R5 Admin Help. See Index > Internet Passwords > Security. The default password scheme is too weak and well-known.
5. Review and restrict Access Control Lists to confirm maximum and appropriate controls. Editing rights and other levels of access are often granted to user classes that do not require the given level of control.

Follow a Mature Software Development Cycle

The quality of software is a reflection of the skill, experience, and processes followed by the individuals that build applications. Be careful selecting software vendors and review their methods prior to beginning work. Does the software team fully document all functionality and security specifications prior to beginning work? Will the development process follow a logical series of stages with clear testing and sign-off procedures to document progress? Are there dedicated or independent staff to test the functioning and security of the application or is the testing done by the same programmer who built the application? These and other due diligence questions will help to assure that the software is being built by a professional and well qualified team of developers.

Third Party Audits

Lotus Notes and Domino Web Server security is a highly specialized field. The developers building the applications are well versed in the construction of functionality but are often not as well informed about the latest security exploits. Outside hackers and security experts are motivated to learn the latest penetration techniques and to apply them in real-world or lab environments.

Experts in breaking systems are also valuable because of their outside perspective. Without any ties to the development of products and code, outside security experts are free to fully exploit any vulnerability without allegiance to the programmer or company that created the software.

Finally, hiring skilled outside auditors will allow a skilled individual to fully mimic the actions of a determined information adversary. Custom applications require custom testing. Automated tools have their place to scan for old documents, misapplied controls or other common problems, however no automated tool can creatively apply individual exploits. Outside security audits and testers can provide a significant mitigation of security risks by testing with a fresh and independent perspective.

CONCLUSION

The strength of the Lotus and Domino web server environment coupled with the flexibility of the system and the ease of application development combine to create a system that can be very secure in theory but often is not secure in practice. Strictly adhering to published security standards, avoiding common mistakes, and evaluating complex applications with independent testing can assure that critical business data is protected. The Lotus Domino environment supports applications that streamline business and increase competitiveness – a balanced security review of these applications insures that the benefits of the environment do not come at the expense of information security.

ABOUT INFOSCREEN

InfoScreen is a professional services firm that works with organizations to devise and sustain an optimal information security risk management program to protect intellectual property and stores of sensitive information. InfoScreen offers application and network penetration testing as well as a comprehensive program of security risk and vulnerability assessment followed by policy implementation and compliance testing.

Contact Information:
InfoScreen, Inc.
118 Prospect Street
Ithaca, NY 14850
(607) 275-0292
www.infoscreen.com