Security Research Advisory

IBM iNotes 9

Active Content Filtering Bypass

Table of Contents

<table>
<tr><td colspan="5">Active Content Filtering Bypass</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-13-01</td></tr>
<tr><td>Severity</td><td>Software</td><td>Versions</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">H</td><td>IBM iNotes</td><td>9</td><td>Remote</td><td>CVE-2013-3032
CVE-2013-3990</td><td rowspan="3">Luca De Fulgentis</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">ibm.com/software/products/inotes</td><td colspan="2"></td></tr>
</table>

Date	Details
07/2013	Vulnerabilities Discovered
07/2013	Vendor Disclosure
08/2013	Security Bulletin Published
08/2013	Public Disclosure

Summary

IBM iNotes is a web based version of the IBM Notes Client software. It interacts with IBM Domino providing collaboration tools using a variety of Web browsers across multiple platforms.

IBM iNotes allows to access Domino-based mail, calendar, schedule, to-do list, contacts, and notebook (Notes Journal) from any web-browser. It uses dynamic HTML and Ajax to provide a rich user-experience while minimizing the number of full-page refreshes and transactions interacting with the Domino web server.

Vulnerability Details

IBM iNotes is prone to **Active Content Filtering (ACF) Bypass**, which results in **Stored Cross-Site Scripting**. The vulnerability could be further employed to realize **Session Hijacking** attacks or to create a **persistent access to the victim mailbox** adding a forwarding rule to an attacker controlled email address by means of **Cross-Site Request Forgery**.

Technical Details

Description

IBM iNotes renders email messages in a browser window realized with HTML elements. To avoid the HTML content eventually present in email messages to interfere with the iNotes interface and logic, it adopts a technology known as *Active Content Filtering (ACF)*.

ACF aims to transform potentially insecure content either by transforming it in harmless content (e.g., comments) or by removing the unsafe portions. IBM iNotes adopts both the techniques:

- Comments JavaScript code specified by the *<script>* tag;
- Strips JavaScript related attributes such as *onclick*, *onmouseover* and similar.

However, it has been found that **for a specific payload, the ACF mechanism fails** to protect the HTML content, allowing an attacker to inject JavaScript content by means of HTML attributes.

Here follows a *proof-of-concept* aiming to exemplify the issue.

HTML code provided as input to IBM iNotes:

```
<img src="< onerror=alert(1)src=x>
```

HTML code obtained as a result:

```
<img < onerror=alert(1) src=x>
```

As shown, in this case the '*src=""*' string has been removed from the HTML code, resulting in an improperly sanitized result which contains the *onerror* attribute that allows an attacker to inject JavaScript code in the iNotes webpage.

To demonstrate the effectiveness of this technique, a real example taken from an HTTP response generated by IBM iNotes is shown in the next page.

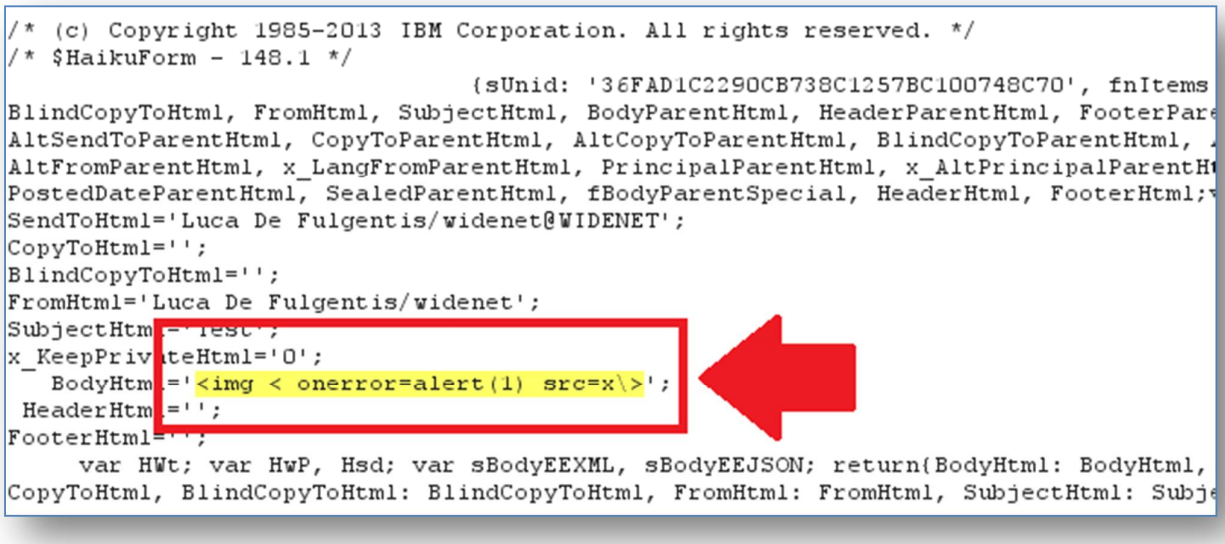

Figure 1 - HTTP response showing the ACF Bypass.

The ACF bypass can be effectively abused to perform stored XSS attacks against iNotes users, as shown in Figure 2.

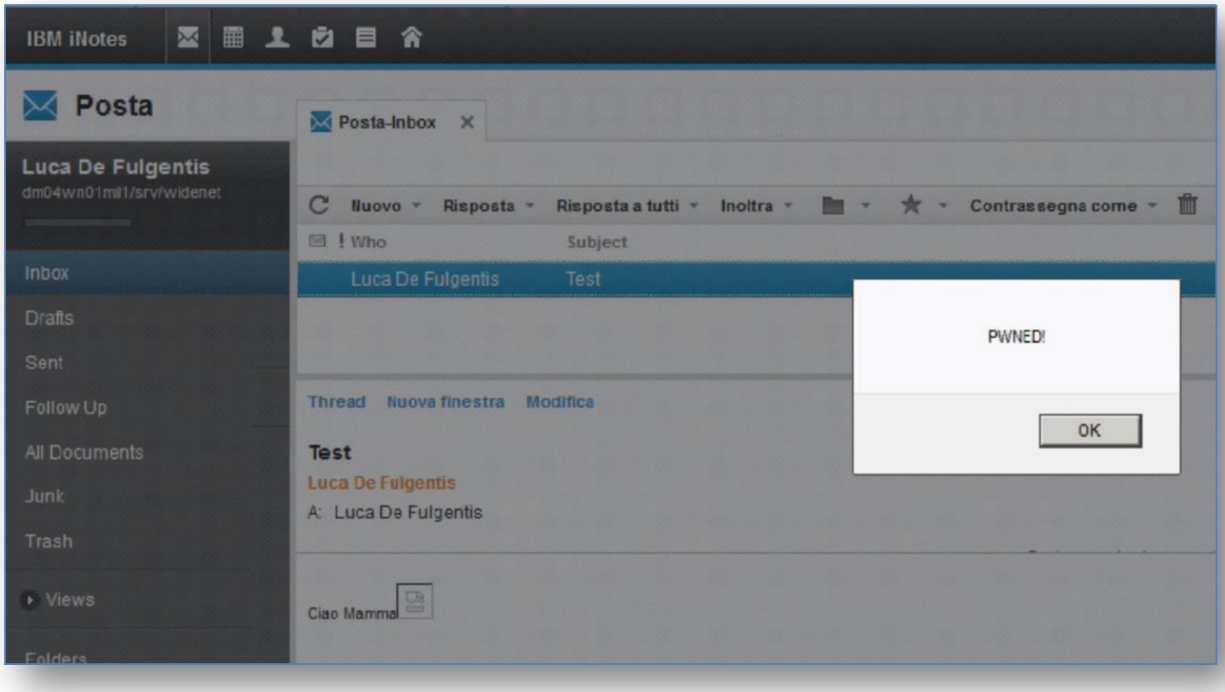

Figure 2 – Stored Cross-Site Scripting against IBM iNotes.

In a real-world attack scenario, the bug could not only be exploited to perform Session Hijacking but also combined with Cross-Site Request Forgery (CSRF) to add a new e-mails forwarding rule to the victim's iNotes application, thus effectively backdooring the victim's mailbox.

As an additional aggravating factor, the mail preview mechanism, if enabled, implies that the victim is not required to open the message in order to trigger the execution of JavaScript code - greatly reducing the required user iteration.

Legal Notices

Secure Network (*www.securenetwork.it*) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41