

[NT] Multiple Vulnerabilities in Mandiant First Response

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Dec 2006 19:22:35 +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>

Multiple Vulnerabilities in Mandiant First Response

SUMMARY

Mandiant First Response is "an incident response tool to collect system information such as running processes, system services, registry information, event logs, and file lists from a local or remote host". The First Response agent (FRAgent.exe) can be installed and configured as a daemon on target hosts in order to collect information remotely via a First Response Command Console. Multiple vulnerabilities exist that could lead to a variety of attack payloads. Agents running in either HTTP or SSL mode are vulnerable to denial of service and server hijacking conditions. The server hijacking vulnerability present in HTTP agents can be further leveraged to allow a rogue process to intercept and modify legitimate agent/console communication, and force a Command Console to download arbitrary content and visit arbitrary URLs.

DETAILS

Vulnerable Systems:

* MFR version 1.1.0 and prior

Immune Systems:

[NT] Multiple Vulnerabilities in Mandiant First Response

* MFR version 1.1.1

Vulnerability #1: Denial of Service against an SSL agent through malformed client requests

When run in daemon mode, the First Response agent (FRAgent.exe) accepts remote connections from a First Response console via HTTP or a modified HTTPS implementation. By sending a series of specially-crafted requests to an SSL-enabled agent, it is possible to force the agent to throw an exception that is not properly handled. After this occurs, the agent's sockets will enter an indefinite CLOSE_WAIT state and all subsequent connection attempts will be refused. The service then must be restarted in order to recover and accept connections again.

Vulnerability #2: Denial of Service against an HTTP or SSL agent through Agent hijacking

An FRAgent daemon permits other processes to bind to the same socket addresses on which it is already listening. If FRAgent is bound to a 0.0.0.0 wildcard address ("all interfaces"), a rogue process can intercept client connections by subsequently binding to the same port on a specific IP address. By hijacking an agent with a non-responsive listener, an attacker can effectively prevent all legitimate client connections.

Vulnerability #3: Command Console and Data Manipulation through HTTP Agent Hijacking

If an HTTP FRAgent daemon is hijacked, the attacker can control the response data sent to and processed by a client, as well as other aspects of client behavior. A rogue process can conduct a man-in-the-middle attack to redirect and modify all requests and responses between the client and a legitimate agent. The attacker can also send specially-crafted HTTP responses that force the client to visit arbitrary URLs and/or download arbitrary content. (NOTE: The use of HTTPS/SSL is default behavior for First Response; using cleartext HTTP requires manual configuration.)

Vendor Response:

Mandiant has confirmed the reports provided by Symantec and updated Mandiant First Response (MFR) to correct these issues. Version 1.1.1 is now available for download from

<http://www.mandiant.com/firstresponse.htm>

<http://www.mandiant.com/firstresponse.htm>. Mandiant advises all users of MFR to upgrade to 1.1.1 as soon as possible. Registered users of the software have been notified via email of availability of the upgrade.

During the course of our review we noted the following addenda to Symantec's analysis:

Vulnerability 1: The DoS condition was due to a design error where the Agent would choose to exit upon receipt of a malformed request. The exit was an explicit choice exercised by the code path and not caused by a buffer overflow or heap corruption. Version 1.1.1 addresses the explicit exit condition and correctly handles requests with malformed payloads, allowing the MFR Agent to continue operation while correctly rejecting

[NT] Multiple Vulnerabilities in Mandiant First Response

malformed requests.

Vulnerability 2 and 3: The vulnerabilities are present because the MFR Agent opens its listening port in non-exclusive mode. Version 1.1.1 correctly opens the port as exclusive, preventing the multiple-bind condition.

Mandiant would like to thank Brian Reilly and Scott King for discovering and notifying us of these vulnerabilities, and Symantec for their participation in public disclosure.

Recommendation:

Upgrade to MFR version 1.1.1, available at <<http://www.mandiant.com/firstresponse.htm>>
<http://www.mandiant.com/firstresponse.htm>.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6475>>
CVE-2006-6475,
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6476>>
CVE-2006-6476,
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6477>>
CVE-2006-6477

ADDITIONAL INFORMATION

The information has been provided by <mailto:brian_reilly@xxxxxxxxxxxxxx>
Brian Reilly.

The original article can be found at:
<<http://www.securityfocus.com/bid/21548>>
<http://www.securityfocus.com/bid/21548>

=====

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@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

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.