Federated Networks Connect Secure Client Agent Vulnerability Assessment

Introduction

BT performed a vulnerability assessment against Federated Network's Connect Secure **Client Agent**. BT utilized standard user access privileges as well as unauthorized techniques to assess the security of the FN Connect Secure Client Agent. The overall purpose of this assessment was to identify application level security issues that could adversely affect or compromise User data protected by the Federated Networks Connect Secure Client Agent, to include, but not be limited to, spyware such as keylogger screen capture tools and Man-in-the-Browser attacks.

BT has extensive experience helping clients secure their application and network infrastructures and evaluate the effectiveness of protections to the loss of intellectual property. Our Security Consultants have helped many of the world's largest institutions protect their Web-based service delivery systems and we have assisted clients that offer electronic commerce solutions. BT's Global Ethical Hacking Center of Excellence (EHCOE) is one of the largest security practices in the world, The team consists of a security community of 1800+ full time client facing consultants / architects / designers, including R&D/V. These industry leading resources that have produced over 20,000 engagements, 100 registered patents, 190 security papers, 108 registered patents. BT is recognized in the industry as "highest capability maturity" by the NSA and "Of the top Three" from Gartner. BT' engagements do not simply perform "scans" of a client's network. We perform highly detailed tests with our proven process and methodologies based from over 20,000 engagements. As not all vulnerabilities fall under the category of a specific published vulnerability, we also employ a proprietary library of manual tests and custom developed tools that are used to check for hard-to-find vulnerabilities, as well as many well-known commercial and public domain tools.

The assessment was conducted by consultants from the BT Ethical Hacking Center of Excellence (EHCOE), an industry leader in protecting business critical information assets.

Description of Testing

At the request of Federated Networks, BT has performed an application vulnerability assessment against the following Federated Networks environments: Federated Networks application identified in the Federated Networks Connect Secure Client Agent Testing Vulnerability Final Report.pdf

The objective of the FN Connect Secure Client Agent Application assessment was to determine the overall security of the application by analyzing all possible transactions, user input variables, and application components that reside on client systems and test the FN connect software for the proper protection against any applicable application-level attacks, to include, but not be limited to, spyware such as a keylogger screen capture tools and Man-in-the-Browser attacks

This type of test includes many of the same testing methodologies that are used during a Web Application Testing Ethical Hacking assessment. However, this type of test focuses on the client with a purpose of attempting to collect as much information as possible about the application and to manipulate the client software without having inside knowledge of how the components operate

BT has developed a customized process for conducting Ethical Hacking assessments of client side applications. This testing is designed to assess the security of the Federated Networks client applications. BT performed a vulnerability testing against the applications to attempt to determine the extent to which an attacker can view, alter, or delete information without proper authorization.

During this testing, BT utilized several test or “dummy” accounts created by Federated Networks for the testing. BT attempted to view and modify information between these test accounts without utilizing the passwords for the accounts. BT also attempted to circumvent assigned user access rights and gain access to functionality not otherwise authorized for access.

Various commercial, publicly available, and BT developed proprietary tools are used during testing and the selection of these tools were entirely at the discretion of BT. Publicly available tools used by BT have undergone a detailed review and evaluation. Review methods include—but are not limited to—validation of functionality, source code review, and sniffer log analysis. Additional testing that was performed utilizing an itemized list of tools provided by Federated Networks. A detailed but obfuscated list of the tools and exploits utilized as part of this test are outline in Appendix A.

Other Federated Networks and third-party vendor systems were beyond the scope of this project

Upon completion of the testing, BT presented all identified vulnerabilities/risks to Federated Networks in a detailed final report. Each vulnerability or risk identified was categorized as *high*, *medium*, or *low*, as follows:

- **High Risk:** These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information.
- **Medium Risk:** These findings identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application, or information, but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, system, application, or information.
- **Low Risk:** These findings identify conditions that do not immediately or directly result in the compromise of a network, system, application, or information, but do provide information that could be used in combination with other information to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. Low risk findings may also demonstrate an incomplete approach to or application of security measures within the environment.
- **Notes:** In addition to Findings, our reports also may contain Notes. Notes can include testing notes, discussions of security best practices, and other supplemental information that may not necessarily be related to the security posture of the systems tested.

Testing Results – Summary Opinion

The vulnerability assessment and testing was performed as outlined above against Federated Network's Secure Connect Application Client, FN Protected WebGoat Application, and Connect Secure Application**.** As part of this assessment, BT presented all findings to Federated Networks in three separate assessment reports. As a result of the testing and verification process completed on November 3, 2010, BT can confirm that there are ***no open High-Risk, no open Medium-Risk, and no open Low-Risk*** vulnerabilities identified at this time. Furthermore, the FN Client Agent completely mitigated all forms of best-of-breed malware such as by way of non-exclusive example a variety spyware tools and methods such as keyloggers, screen capture tools and Man-in-the-Browser attacks, as outlined in greater detail in Appendix B.

Cautionary Note

The application assessments that BT performed was based on past experiences, currently available information, and known threats as of the date of testing. Given the constantly evolving nature of information security threats and vulnerabilities, there can be no assurance that any assessment will identify all possible vulnerabilities, or propose exhaustive and operationally viable recommendations to mitigate those exposures.

The statements relevant to the security of the Federated Networks applications in this letter reflect the conditions found at the completion of testing.

In accepting our report on the Federated Network's Secure Connect Application Client, FN Protected WebGoat Application, and Connect Secure Application, Federated Networks has acknowledged the validity of the above cautionary statement. BT also strongly recommends that any network, information system, or online application be subject to periodic reassessment and policy review, in addition to complementary training of the key support personnel on such policies and procedures for the above infrastructure in order to maintain a strong security profile in the face of potential threats.

Appendix A

BT employed a variety of automated and manual tools to increase the thoroughness of the analysis and to increase efficiency.

Tool #	Attack Scenario	Threat Mitigated
1	Man In The Middle/Sniffing Attack/Pharming	✓
2	Sniffing Attacks/ Replay Attack	✓
3	Sniffing Attacks/Man In The Middle	✓
4	Sniffing Attacks	✓
5	Man In The Middle Attack/Sniffing Attack	✓
6	Sniffing Attack	✓
7	Memory Forensic/Screen Capture/Keylogging	✓
8	Screencapture/ Keylogging	✓
9	Memory Forensics	✓
10	Keylogging	✓
11	Screencapture	✓
12	Screen Capture	✓
13	Keylogging	✓
14	Screen Capture	✓
15	Memory Forensics	✓
16	Keylogging	✓
17	Keylogging, Screen Capture	✓
18	Keylogging	✓
19	Known Credential Attack/MITM	✓
20	Screen Capture	✓
21	Hardware Keylogging	✓
22	Keylogging	✓
23	Keylogging	✓
24	Man In The Middle Attack/Sniffing Attack	✓
25	Memory Forensics	✓
26	Screen Capture/Recording	✓
27	Keylogging	✓
28	Screen Capture/Keylogging	✓