GoodSecurity Penetration Test Report

Andrew Anelli [HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com" HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com" HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com" HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com" HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com" HYPERLINK "mailto:YOURNAMEHERE@GoodSecurity.com"@GoodSecurity.com](mailto:YOURNAMEHERE@GoodSecurity.com)

10/12/2021

* High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp’s CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans’ computer and determine if it is at risk. GoodSecurity’s overall objective was to exploit any vulnerable software and find the secret recipe file on Hans’ computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were

identified on Hans’ desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the ‘Findings’ category.

* Findings

Machine IP:



Hostname:



Vulnerability Exploited:



Vulnerability Explanation:

The Icecast application running on 192.168.0.20 allows for a buffer overflow exploit. An attacker can remotely gain control of the victim’s system by overwriting the memory on the system, which writes past the end of a pointer array when receiving 32 HTTP headers.

Severity:

this would be a very severe issue. File discovery and exfiltration, key logging and screen capture, privilege escalation to Administrator can all be done via this vulnerability.

The system was also found to be vulnerable to the following exploits:

exploit/windows/local/ikeext\_service

exploit/windows/local/ms16\_075\_reflection

Proof of Concept:

















/ms16\_075\_reflection: Module utilizes the Net-NTLMv2 reflection between DCOM/RPC to achieve a SYSTEM handle for elevation of privilege. Currently the module does not spawn as SYSTEM, however once achieving a shell, one can easily use incognito to impersonate the token. This will also allow the attacker full access to the system.

/ikeext\_service: A windows program looks for DLLs when it starts. If these DLL’s do not exist then it is possible to escalate privileges by placing a malicious DLL in the location where the application is looking for. This will also allow the attacker full access to the system.

* Recommendations

The first step is to update the Icecast software to a current version that will not be vunerable to this type of attack. The second step would be to update the Windows OS to prevent the use of the above mentioned exploits. These two steps would prevent the attacker from gaining original access via the Icecast system and prevent the elevation of privilege issues caused by the two noted exploits.