Institute of Computer Science
Computer Security MTAT.03.134

CVE-2014-2034

Author: Hans Raukas
Instructor: Meelis Roos

Tartu 2014
Introduction

Sonatype is a corporation with many contributions to the open source community, one of them being Nexus Repository Manager. Nexus provides development teams the ability to proxy remote repositories and share software artifacts. Recently a critical security vulnerability was discovered by an external researcher. The REST API vulnerability made use of an unauthenticated execution path that allowed creation of user accounts in Nexus OSS/Pro versions from 2.4.0 to 2.7.1.

Summary

With the REST API vulnerability the Nexus could be compromised, allowing an attacker to escalate a session and create user accounts. The accounts created by the attacker could receive any privileges, including administrative privileges, without requiring any sort of user authentication. These accounts could be created by the attacker in any running instance of Nexus, although internet accessible instances of Nexus had a more severe chance of coming under attack due to being accessible by large audience opposed to the more limited audience associated with non-Internet accessible instances. The attacker could then use the account to perform any actions based on the privileges assigned to that user account. For example, an attacker could make an account, assign administrative privileges to it and then use it to manipulate (e.g. change, delete) the contents of the Nexus repository.

Solution

To fix the security vulnerability that was confirmed in Nexus versions 2.4.0 through 2.7.1 Sonatype released an updated version of Nexus (version 2.7.2), but also released patches for the previously mentioned affected versions of Nexus. With the release of Nexus 2.7.2 and the patches for the earlier affected versions a mitigating control was added that improved the security of the system and closed the loophole through which the attacker could gain access to the system unauthorized. In addition to that, SSL (Secure Socket Layer) support was also added in the current latest version.
2.8.0 which provides the ability to secure access to the Nexus user interface and content via https and also to the Central Repository that the Nexus Repository Manager uses. With these changes Nexus is currently considered safe from being accessed without user authorization and thus being safe from the REST API vulnerability.

(Extended Validation and Standard SSL Certificate indicators)

Bibliography

http://www.sonatype.org/
https://support.sonatype.com/entries/42374566-
https://support.sonatype.com/entries/23150053-Sonatype-Nexus-Release-Notes
http://www.sonatype.com/nexus/why-nexus-pro/nexus-pro-features
http://www.sonatype.com/clm/secure-access-to-central
https://wwwglobalsign.eu/ssl-information-center/what-is-ssl.html