

2021-07-21 Jira (software, service management) Security Advisory

漏洞-CVE-2020-36239

只影响JIRA DataCenter版本

主题	CVE-2020-36239- 缺少Ehcache RMI的身份验证
安全信息发布时间	21 Jul 2021
涉及产品	• Jira Data Center • Jira Software Data Center • Jira Core Data Center • Jira Service Management Data Center JIRA的server版本不受影响 JIRA的Cloud版本不受影响
影响Confluence版本	Jira Data Center, Jira Core Data Center, and Jira Software Data Center • 6.3.0 <= version < 8.5.16 • 8.6.0 <= version < 8.13.8 • 8.14.0 <= version < 8.17.0 Jira Service Management Data Center • 2.0.2 <= version < 4.5.16 • 4.6.0 <= version < 4.13.8 • 4.14.0 <= version < 4.17.0 Jira Data Center, Jira Core Data Center, and Jira Software Data Center • All 6.3.x, 6.4.x versions • All 7.0.x, 7.1.x, 7.2.x, 7.3.x, 7.4.x, 7.5.x, 7.6.x, 7.7.x, 7.8.x, 7.9.x, 7.10.x, 7.11.x, 7.12.x, 7.13.x versions • All 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x versions • All 8.5.x versions before 8.5.16 • All 8.6.x, 8.7.x, 8.8.x, 8.9.x, 8.10.x, 8.11.x, 8.12.x versions • All 8.13.x versions before 8.13.8 • All 8.14.x, 8.15.x, 8.16.x versions Jira Service Management Data Center • All 2.x.x versions after 2.0.2 • All 3.x.x versions • All 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x versions • All 4.5.x versions before 4.5.16 • All 4.6.x, 4.7.x, 4.8.x, 4.9.x, 4.10.x, 4.11.x, 4.12.x versions • All 4.13.x versions before 4.13.8 • All 4.14.x, 4.15.x, 4.16.x versions
修复版本	Jira Data Center, Jira Core Data Center, and Jira Software Data Center • Version 8.5.16 for 8.5.x LTS • Version 8.13.8 for 8.13.x LTS • Version 8.17.0 Jira Service Management Data Center • Version 4.5.16 for 4.5.x LTS • Version 4.13.8 for 4.13.x LTS • Version 4.17.0

解决方案

我们建议升级版本

升级到Jira Data Center, Jira Core Data Center, Jira Software Data Center指定版本

- 8. 5. 16
- 8. 13. 8
- 8. 17. 0
- 更高版本

Jira Service Management Data Center to versions升级到指定版本

- 4. 5. 16
- 4. 13. 8
- 4. 17. 0
- 更高版本

或者

通过使用防火墙或类似技术，将对Jira Data Center, Jira Core Data Center, and Jira Software Data Center和JJira Service Management Data Center的Ehcache RMI端口的访问限制为仅对集群实例的访问。

即，端口只开放给Data Center的结点服务器

安全漏洞描述

Jira Data Center, Jira Core Data Center, and Jira Software Data Center和JJira Service Management Data Center暴露了一个Ehcache RMI网络服务，攻击者可以连接到该服务的端口40001和40011[0][1][2]上，由于缺少身份验证漏洞，可以通过反序列化在Jira中执行他们选择的任意代码。Atlassian强烈建议仅将对Ehcache端口的访问限制为数据中心实例，而Jira的固定版本现在将需要共享机密，以便允许访问Ehcache服务。

[0] Jira Data Center, Jira Core Data Center, and Jira Software Data Center 7.13.1之前的版本中，可以随机分配Ehcache对象端口。

[1] 在3.16.1之前的JJira Service Management Data Center中，Ehcache对象端口可以随机分配。

[2] 默认的Ehcache端口是40001，但可以将其配置为位于不同的端口上