PTA CERT for Telecom Sector

Security Advisory-No: 27

2nd , Nov 2018

Threat Classification: Vulnerability

Name of vulnerabilities:

- Security Restriction Bypass Vulnerability
  (CVE-2016-9843, CVE-2018-3529, CVE-2018-11776, CVE-2018-1258)

Distribution: The vulnerabilities can be exploited in the following product versions:

- Java VM component of Oracle Database Server **(11.2.0.4, 12.1.0.2, 12.2.0.1, 18c)**
- MySQL Server component of Oracle MySQL **(5.5.61, 5.6.41, 5.7.23, 8.0.12 & prior)**
- MySQL Enterprise Monitor component of Oracle MySQL **(3.4.9.4237,4.0.6.5281,8.0.2.8191 & prior)**

Exploited Vulnerabilities:

CVE-2018-3529: Vulnerability could allow the unauthenticated attacker with network access via multiple protocols to compromise Java VM. On successful exploitation, attackers could gain access to Java VM.

CVE-2016-9843: Vulnerability could allow the low privileged attacker with network access via multiple protocols to compromise MySQL Server. On successful exploitation, attackers could gain access to the MySQL Server.

CVE-2018-11776: Vulnerability could allow the unauthenticated attacker with network access via HTTP to compromise MySQL Enterprise Monitor. On successful exploitation, attackers could gain access to MySQL Enterprise Monitor.

CVE-2018-1258: Vulnerability could allow the low privileged attacker with network access via HTTP to compromise MySQL Enterprise Monitor. On successful exploitation, attackers could gain access to MySQL Enterprise Monitor.

Recommendations:

1) Registered users may use following official patches to fix aforementioned vulnerabilities:
   - https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
2) Only use licensed software and avoids download/use of cracked and pirated software.
3) Designate a PoC for your network users for seeking assistance and reporting security issues.
4) In case of any incident, please report to this office.