PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

24 August 2017
S1: 300384354/pbsa56

Security Advisory for mGuard Device Manager, mdm

Synopsis

Multiple security issues and vulnerabilities in Oracle Java SE possibly affecting mGuard Device Manager.

Affected products

PHOENIX CONTACT FL MGUARD DM (mGuard Device Manager, mdm) 1.8.0 and older.
The mGuard Device Manager is a software product that is based on Java Technology. The necessary Java software is bundled with the mGuard Device Manager Windows installer. The security issues and vulnerabilities are within this Java software.

Mitigation

All users of the affected product on Windows should update to at least version 1.8.0.1. The update can be performed by simply executing the installer for version 1.8.0.1 on a Windows system where the product is installed in version 1.8.0. The installer is available for download at: https://phoenixcontact.com/product/2981974 in the Downloads/Software section.
For more information please refer to the document “How to upgrade mGuard device manager” downloaded with the installer.
All users of the affected product on Linux should also update Java to the latest version. When using the packet source delivered by PHOENIX CONTACT on Ubuntu this is simply done by using the software updater of the operating system.

Issues

Cited from the original report from Oracle with respect to Java SE (Standard Edition):

CVE-2017-10102: Vulnerability resulting in takeover of Java SE.
“Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. […] attacks may significantly impact

additional products. Successful attacks of this vulnerability can result in takeover of Java SE [...].”

CVE-2017-10116: Vulnerability resulting in takeover of Java SE.
“Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks require human interaction from a person other than the attacker and […] may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE [...].”

CVE-2017-10078: Unauthorized access to critical Java SE data.
“Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data as well as unauthorized access to critical data or complete access to all Java SE accessible data.”

CVE-2017-10115: Unauthorized access to critical Java SE data.
“Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE […] accessible data.”

CVE-2017-10118: Unauthorized access to critical Java SE data.
“Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE […] accessible data.”

CVE-2017-10176: Unauthorized access to critical Java SE data.
“Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE […] accessible data.”

CVE-2017-10198: Unauthorized access to critical Java SE data.
“Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. [...] attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE [...] accessible data.”

CVE-2017-10135: Unauthorized access to critical Java SE data. “Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE […] accessible data.”

CVE-2017-10053: Partial denial of service of Java SE.
“Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks of this vulnerability can

result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE [...].”

CVE-2017-10108: Partial denial of service of Java SE.
“Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE [...]. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE [...].”