RiskBased SECURITY

RBS-2019-013

Danfoss AK-EM 800 Multiple Vulnerabilities

Table of Contents

Vendor / Product Information

Danfoss is a major engineering company founded in Denmark but now operating factories and offices worldwide. The company serves many different markets including the food retail industry to which their AK-EM 800 product is offered. This is an Enterprise Management solution with a central architecture function providing alarm management, automatic data collection, together with food quality reporting.

Vulnerable Program Details

Details for tested products and versions:

Vendor:	Danfoss
Product:	AK-EM 800
Version:	2.24

NOTE: Other versions than the one listed above are likely affected.

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

Danfoss AK-EM 800 provides a web-based management interface in which multiple remote vulnerabilities were discovered. The most severe allows remote backdoor access to the system with super administrator privileges. Various local vulnerabilities were also discovered related to improper permissions that allow disclosure of credentials or privilege escalation.

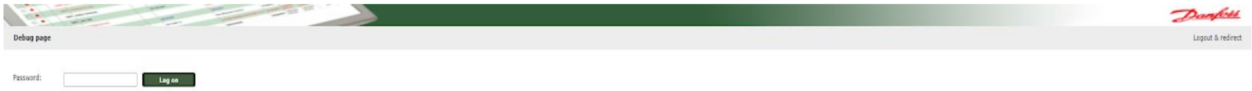
Overall, there are no local security boundaries in vulnerable versions and while not stated anywhere in the product documentation, the software should only be installed on secured systems with trusted users. Similarly, as the product does not honour least privilege security recommendations, any remote compromise would lead to complete control over the system with SYSTEM privileges.

Vulnerability Details

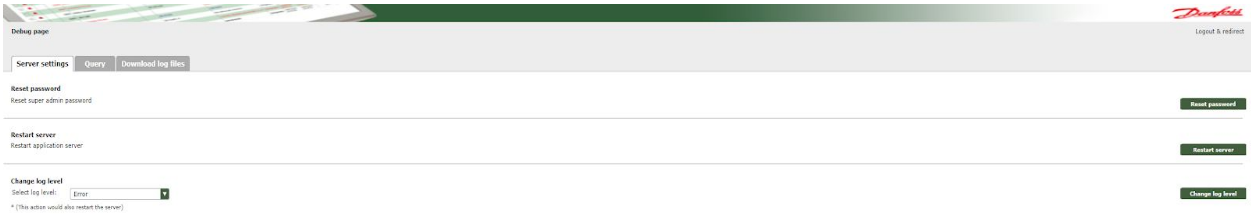
Undocumented Debug Service Predictable Password Remote Backdoor

The web-based management interface provides access to an undocumented debug service. This seems to be intended for the vendor to access customers' systems if support is required.

The debug interface is accessed via the following URL:
http://[IP]:8080/AKEM_800/#login/debug



Access to the debug interface is password restricted. The password is not stored anywhere but dynamically generated. Unfortunately, this is done in a predictable manner based on the system date. This allows a remote attacker to trivially generate the correct password and log into the debug interface.



Reset password
Reset super admin password

Restart server
Restart application server

Change log level
Select log level: Error
* (This action would also restart the server)

From here the attacker can e.g. change the log level, restart the server, or download log files. More importantly the attacker can also reset the hardcoded super administrator account's password to 'danfoss' or execute arbitrary SQL queries to disclose or update data in the underlying database.

LogFilesDownloadServlet Unauthorized Remote Access

One of the servlets provided by the undocumented debugging feature is downloadLogFiles. This servlet serves two purposes as controlled by the 'queryOrdownload' parameter: downloading of log files or executing SQL queries passed via the 'queryParam' parameter and returning the results to the user.

This functionality is only intended to be accessible to the debug backdoor account once successfully authenticated. However, due to missing authentication checks in the servlet it is possible for unauthenticated, remote attackers to access the functionality via direct requests.

The following request returns all user account information:
http://[IP]:8080/AKEM_800/ak_em_800_1_0/downloadLogFiles?queryParam=Select * from ak_em_800_db.tbl_user_info_new&queryOrdownload=query

Web Interface User Authentication Account Lockout Remote DoS

The web-based management interface implements a mechanism to reduce the risk of password brute forcing. Instead of relying on throttling or temporary lockouts, which are common approaches, it does a hard lockout of an account after five consecutive failed login attempts. Locked accounts require the assistance of an administrator to manually get unlocked.

This approach is generally considered problematic. It effectively allows remote attackers to cause a denial of service by locking out accounts and thus preventing them from accessing the service. It is possible to lock out any account including the default "admin" super administrator account.

As a side note, this also allows enumerating valid user accounts. If an attacker fails to log in five times with an invalid account, no account lockout message is displayed, whereas one is displayed if the account is valid. Obviously, once an attacker has determined a valid account that account is locked, so the impact of the user enumeration is limited.

Insecure Default Permissions Local Privilege Escalation

Danfoss AK-EM 800 installs with insecure default permissions that allow unprivileged user accounts to place arbitrary files in the installation path or replace existing files including executables and DLL files.

As the software has multiple services running with SYSTEM privileges, this may allow a local attacker to execute arbitrary code with these privileges. One attack vector involves planting a trojan DLL file named msvcrt71.dll in the AKEM_800\jre\bin\server directory. The next time the service is started, the code in the malicious DLL file is executed with SYSTEM privileges.

Multiple Files Insecure Default Permissions Local Credential Disclosure

During installation of the product, a super user account is created. The credentials for this account are stored in cleartext within the following two files with world-readable permissions:

1) %HOMEDRIVE%\AKEM_800\installationInfo\AKEM_Installation_logger.txt
2) %HOMEDRIVE%\AKEM_800\db\bin\AddUserToSqlDb.sql

This may allow a local attacker to trivially disclose the credentials and log into the MySQL service or web-based management interface as a privileged account.

Other Discoveries

During the review of the AK-EM 800 software we noticed various other security-relevant issues. These are either concerns or poor security practices that are not considered outright vulnerabilities or related to the use of vulnerable 3rd party components.

Web Interface Default Credentials

Danfoss AK-EM 800 installs four default user accounts ('admin', 'administrator', 'user', and 'guest') with a default password of 'danfoss'. While this is publicly known and documented in the user guide, default accounts are considered bad security practice. In this case, the accounts cannot be disabled. While a user is asked to change the default password for the account when logging in for the first time, there is a risk that system administrators may not log in as each account and change the default password. If they fail to do so, a remote attacker may trivially gain access to the web-based management interface.

Unsafe Third Party Components

The latest version includes many older third party components with known vulnerabilities. These include MySQL version 5.1.53 from 2010, which runs with SYSTEM privileges and is remotely accessible, Tomcat version 7.0.57 from 2014, which also runs with SYSTEM privileges, as well as many different Java libraries.

Solution

The vendor has released version 2.33, which addresses all listed vulnerabilities. The bundled version of Tomcat has also been updated. Other vulnerable 3rd party components are scheduled for updating later in the year.

References

RBS:	RBS-2019-013[1]
VulnDB:	208859, 208860, 208861, 208862, 208863, 208864

Timeline

2018-10-29	Vulnerabilities reported to the vendor.
2018-10-29	Vendor response received.
2019-07-15	Alert sent to RBS VulnDB clients.
2019-09-03	Vendor releases updated version.
2019-09-03	Publication of this vulnerability report.

[1] https://www.riskbasedsecurity.com/research/RBS-2019-013.pdf

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.