Ellipse8 Security Vulnerability

ABBVU-PSSW-201703

Update Date: *11/21/2017*

Notice

Affected Products

Ellipse 8.3 – Ellipse 8.9 (including Ellipse Select)

Vulnerability ID

ABB ID: ABBVU-PSSW-201703

Summary

ABB is aware of a security vulnerability in the product versions listed above.This would require the attacker to have access to the local network.

An attacker who successfully exploited this vulnerability could discover authentication credentials by sniffing network traffic. ABB is providing resolution to this vulnerability with product release versions 8.5.26 - 8.9.6 that will be made available December 5-7, 2017. ABB strongly recommends that customers apply the update as soon as they are able.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for CVSS v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

Note: This is not a vulnerability specific to Ellipse, but rather risk introduced by the implementation of LDAP. The CVSS score reflects this risk.

CVSS v3 Base Score: 6.5

CVSS v3 Temporal Score: 6.0

CVSS v3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C/CR:H:

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0

Corrective Action or Resolution

ABB is providing resolution to this vulnerability in order to provide adequate protection to customers. The problem is corrected in the following product versions:

Ellipse 8.5.26	Release 7 Dec 2017
Ellipse 8.6.21	Release 5 Dec 2017
Ellipse 8.7.18	Release 7 Dec 2017
Ellipse 8.8.12	Release 7 Dec 2017
Ellipse 8.9.6	Release 7 Dec 2017

ABB is currently working on a solution for customers that deploy Ellipse 8.3/4. If a customer has plans to upgrade, the vulnerability will be address in that version. ABB will notify the Ellipse 8.3/4 customers once it is determined whether a solution is available on their release or whether an upgrade will be required.

ABB strongly recommends that customers apply the update as soon as they are able.

Vulnerability Details

A vulnerability exists in the authentication of Ellipse to LDAP/AD using the LDAP protocol included in the product versions listed above. An attacker could exploit the vulnerability by sniffing local network traffic and discovering authentication credentials.

A change has been made to the affected Ellipse versions to secure this authentication over LDAPS between the Application Server and the LDAP/AD server.

Note: an attacker would first have to gain access to the local network in order to exploit this vulnerability.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

Enabling LDAPS authentication on the Ellipse Appliance

Introduction

Ellipse performs external host authentication by using the LDAP protocol for communication with Active Directory or other Directory Services. Standard LDAP traffic (port 389) is not encrypted, and sensitive account information travel between the Ellipse application server and the LDAP server. A change is required to support encryption of authentication information traveling between Ellipse and the External Authentication Service. Please note, this technical note does not cover encryption of traffic between Ellipse and Web Clients, for which support of SSL encryption is already available and documented.

Implementation (Appliance)

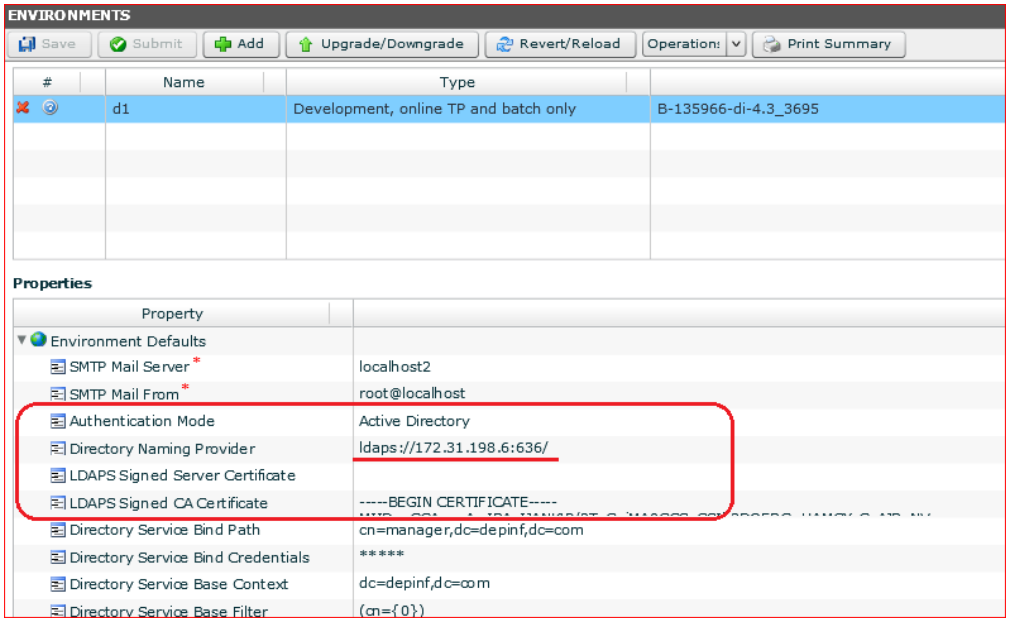
JBOSS has the ability to establish an LDAPS secure connection with AD, provided that an SSL certificate is shared between the authentication server implementing LDAP and Ellipse.
A change was made to the Deployment Infrastructure code running on the appliance so that a certificate (and optional CA chain certificate) can be entered as an Environment parameter in VEAM and passed to the JBOSS server running Ellipse, via the appliance's internal automation.
Following, steps required to implement this solution. Please note, a manual procedure step is also provided for those customers who require LDAPS encryption but haven't updated their appliances to the latest infrastructure.

Step 1: Enable LDAPS on the Active Directory service, "Directory Naming Provider" (common)

The AD domain controller (or other directory service) will need to be loaded with a valid certificate and private key. Documentation of that step is out of scope of this document. A good guide is the following link.
https://www.petri.com/enable-secure-ldap-windows-server-2008-2012-dc
Please note: similarly to the standard LDAP implementation, LDAPS handshaking over SSL occurs only between the Ellipse server and an LDAP server specified in the "Directory Naming Provider" field.

Step 2: Add certificate to environment properties in VEAM (automatic procedure)

Two new text fields are now available in VEAM, both at the Site and Environment level. Similar to the SSL certificates needed to enable HTTPS traffic, these fields are plain text, and should be loaded with PEM, Base64 encoded certificates. Please note: unlike SSL Server Certificates for HTTPS, a private key is not required for the handshaking.



Please note that the Directory Naming provider will need to reflect the new LDAPS URL. Standard port for LDAPS traffic is normally 636.
The certificate text is to be entered as standard Base64 encoding (PEM format), the same as the standard HTTPS certificates used for Ellipse.
Once these parameters are set, an environment should be redeployed to make sure Ellipse can establish an encrypted LDAPS connection.

Step 2 alt: Add certificate to JBOSS (manual procedure)

This procedure should be performed when VEAM support for LDAPS certificates is not available but LDAP traffic encryption is required.

- In VEAM, enter the "ldaps:" URL, as shown in the screenshot before, even if the LDAPS certificate fields are not shown.
- Save and Submit, to redeploy the environment.
- Once the Ellipse servers are deployed, use your file transfer method of choice to transfer the certificate(s) to the Ellipse virtual server, in PEM format.
- Connect to the Ellipse server, and issue the following commands to load the certificates to the Java keystore:
    - service ellipse stop
    - export JAVA_HOME=/usr/java/default
    - export PATH=$JAVA_HOME/bin:$PATH
    - keytool -importcert -file [*path_to_cert_file]* -keystore *$JAVA_HOME/jre/lib/security/cacerts -storepass changeit -noprompt -alias ldaps*

- *(repeat for CA certificate if required)*
- service ellipse start

Troubleshooting

In general, to troubleshoot Ellipse LDAPS issues, the following steps should be performed on the Ellipse VM experiencing failures.

1- Add option " -Djavax.net.debug=ssl,handshake" to JAVA_ARGS in the JBOSS options definition file, /etc/jboss-as/ellipse.conf
2- Restart JBOSS
3- Reproduce the Login Error
4- Collect diagnostic information by running CSI gather
5- Send to ABB for further analysis

Conclusion

This concludes the steps required to implement encrypted LDAP handshaking. Implementing the solution involves a step to enable LDAPS by uploading and sharing a known certificate.
Implementation and troubleshooting requires a good knowledge or Active Directory, the Domain Controller, and supported protocols.
It is important to note that this solution is only to enable encryption between the Ellipse Server and the Directory Naming service and does not change or enhance the information exchange between the two parties in any way or form.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could discover authentication credentials by sniffing local network traffic between Ellipse and the LDAP/AD server.

What causes the vulnerability?
The vulnerability is caused by the use of unsecured protocols between Ellipse Application Server and the LDAP/AD Server

What is the affected product?
Ellipse 8.3 – Ellipse 8.9 (including Ellipse Select)

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability log in to network systems with stolen credentials.

Could the vulnerability be exploited remotely?
No, to exploit this vulnerability an attacker would need to have to the local network.

What does the update do?
The update removes the vulnerability by modifying the way that the Ellipse Application will use LDAPS for authentication.

When this security advisory was issued, had this vulnerability been publicly disclosed?
No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?
No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued

Support

For additional information and support please contact your local ABB service organization. For contact information, see http://new.abb.com/enterprise-software/services/maintenance/support.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.