



Security Alert Update

OpenText™ EasyLink Electronic Data Interchange (EDI) Services may be vulnerable to the Padding Oracle on Downloaded Legacy Encryption (POODLE) threat.

Please review this alert to determine whether your site is vulnerable and learn how to mitigate this vulnerability.

Systems Affected

- EasyLink ICCNet
- EasyLink GMS

Details

One of the protocols used by EasyLink EDI Services to establish a secure sockets connection may be vulnerable to the POODLE threat (CVE-2014-3566).

Impact

Any service or client that supports Secure Sockets Layer (SSL) version 3 (SSLv3) can be exploited so that an attacker can decrypt secure sessions, revealing passwords and other private information.

Solution

OpenText will disable SSLv3 to prevent it from being used to access EasyLink EDI Services. Instead, OpenText will use TLS 1.0, which is the recommended protocol to safeguard against POODLE attacks. Remediation activities will be performed as outlined in the table below.

Date/Time	Affected Systems
Tuesday, Sept 1st, 2015 8:00AM (ET)	EasyLink GMS Web Administration Tool EasyLink ICCNet B2B Management Center EasyLink ICCNet Web Applet The following DNS/IP Addresses will disable SSLv3: gmsadmin.easylink.com / 165.251.36.199 b2b.easylink.com / 165.251.195.227 vanclient.easylink.com / 165.251.195.12
Tuesday, Sept 15th, 2015 8:00AM (ET)	EasyLink ICCNet WEB APPLET/FTP Services EasyLink ICCNet AS2 Services The following DNS Addresses will disable SSLv3: mft.easylink.com / 165.251.195.10 (both applet and ftp) vanclient01.easylink.com & vanftp01.easylink.com / 165.251.195.4 (both applet and ftp) vanclient02.easylink.com & vanftp02.easylink.com / 165.251.195.5 (both applet and ftp) vanconnect.easylink.com / 165.251.195.7 (AS2)
Tuesday, Sept 29th, 2015 8:00AM (ET)	EasyLink GMS FTP Services EasyLink GMS AS2 Services The following DNS/IP Addresses will disable SSLv3: paau.ps.easylink.com & ftps1.easylink.com / 165.251.36.130 (ftp) vaau.ps.easylink.com & ftps2.easylink.com / 165.251.36.131 (ftp) psau.ps.easylink.com & ftps3.easylink.com / 165.251.36.5 (ftp) ediin.easylink.com / 165.251.36.200 (AS2)

To avoid any disruption in service, OpenText recommends that customers disable SSLv3 and enable TLS 1.0 or higher in their web browser. Additionally, customers will need to ensure that their API integrations to other applications support TLS 1.0 or higher.

Exception Listing

Although OpenText recommends disabling SSL as the most effective way to address the POODLE threat, we understand that not all customers can support TLS. If you are unable to support TLS, OpenText has established an exception listing that will allow customers to continue to access the EasyLink network using SSL. In order to enable your continued use of SSL, you will be required to [visit our website](#) to add your company to our exception listing.

More Information

For more information, contact EasyLink EDI Support.

Phone: 1-800-209-6245 / 1-678-823-4600 (local)

Email EasyLink GMS Support: irf@easylink.com

Email EasyLink ICCNet Support: vanhelp@easylink.com

Copyright ©2015 Open Text Corporation. All Rights Reserved. OpenText is a trademark or registered trademark of Open Text SA and/or Open Text ULC. The list of trademarks is not exhaustive of other trademarks, registered trademarks, product names, company names, brands and service names mentioned herein are property of Open Text SA or other respective owners. All rights reserved. For more information, visit: <http://www.opentext.com/2/global/site-copyright>.