Visa Security Alert

NOVEMBER 2017

CYBERCRIMINALS LEVERAGING DYNAMIC DATA EXCHANGE PROTOCOL

Distribution: Issuers, Acquirers, Processors and Merchants

Summary: On 8 November, Microsoft issued Security Advisory 4053440 providing guidance on securing Microsoft applications when processing Dynamic Data Exchange (DDE) fields. The DDE protocol enables messages to be sent between Microsoft applications and uses shared data to be sent between applications. Visa notes that a malicious cyber actor could leverage the DDE protocol when delivering specially crafted files to users through phishing and web-based downloads, and strongly recommends that users exercise caution when opening suspicious files.

Visa Payment Systems Intelligence is aware of multiple cybercriminal threats to the payments ecosystem currently leveraging DDE protocol in phishing campaigns. The primary cybercriminal exploitation method begins with a phishing e-mail and relies on the Dynamic Data Exchange (DDE) protocol for infection instead of malicious macros or an exploit kit. Visa is providing this alert to ensure awareness of the cyber threats actively exploiting this Microsoft Windows feature. In their advisory, Microsoft provides controls and mitigations regarding the DDE protocol.

About DDE Protocol

According to Microsoft, Microsoft Office provides several methods for transferring data between applications. The DDE protocol is a set of messages and guidelines. It sends messages between applications that share data, and uses shared memory to exchange data between applications. Applications can use the DDE protocol for one-time data transfers and for continuous exchanges in which applications send updates to one another as new data becomes available.

1. Microsoft Security Alert and Attack Scenario

Microsoft provides information regarding security settings for Microsoft Office applications and guidance on what users can do to secure Microsoft applications when processing DDE fields. Microsoft Office applications include the DDE feature, which allows one Microsoft document to access data from another document. This is a useful functionality; however, the document field requesting data can be altered to include execution of arbitrary commands, including the commands to download and execute malicious payloads

The advisory describes the general attack scenario in which an attacker could leverage the DDE protocol by sending a specially crafted file to the user and then convincing the user to open the file. In the process, the attack would have to convince the targeted user to disable Protected Mode and click through one or more additional prompts. With phishing being one of the primary attack methods used by malicious actors to target victims, Microsoft strongly recommends that customers exercise caution when opening suspicious file attachments.

2. Microsoft Security Guidance, Best Practices, and External Resources

Microsoft Security Guidance

Microsoft strongly encourages all Microsoft Office users to review the security-related feature control keys and to enable them. Additionally, Microsoft provides further details and warnings regarding various steps that users can take to protect themselves. Please refer to the Microsoft Security Advisory for further information. Additional Microsoft discussion on using DDE can be found here.

Best Practices

Visa recommends the following best practices to reduce the risk of exposure:

a. Educate employees about avoiding phishing scams and safely opening emails with attachments
b. Turn on heuristics (behavioral analysis) on anti-malware to search for suspicious behavior
c. Refer to the external resources below for more information on security and best practices
d. Refer to Visa's What to do if Compromised (WTDIC) document, published August 2016

External Resources

- Microsoft Security Advisory 4053440
- Microsoft Office 2016: Secure and control access to Office
- Microsoft Office 2013: Secure Office 2013

To report a data breach, contact Visa Fraud Control:
Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
Europe: Datacompromise@visa.com
LAC: LACFraudInvestigations@visa.com
U.S. and Canada: USFraudControl@visa.com

For more information, please contact, paymentintelligence@visa.com.