National Cyber Security Centre

2003240928-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Advisory

Type 1 Font Parsing Remote Code Execution Vulnerability
2020-03-24

Status: TLP-WHITE

NCSC

Traffic Light Protocol

This document is classified using Traffic Light Protocol. Recipients may share TLP: WHITE information freely, without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. **Please treat this document in accordance with the TLP assigned.**

Technical Detail

1. Overview

Threat Type	Remote code execution vulnerability in Adobe Type Manager Library.
Systems Affected	All currently supported versions of Windows and Windows Server operating systems.
Impact	Successful exploitation of the vulnerability would grant the attacker control of an affected system.
Recommendations	CSIRT-IE recommends that users take defensive measures to minimise the risk of exploitation of this vulnerability. Specifically, users should: • Review the Microsoft Advisory ADV200006 • Apply the relevant workaround.

2. Description

Microsoft has released a security advisory to address remote code execution vulnerabilities in Adobe Type Manager Library affecting all currently supported versions of Windows and Windows Server operating systems. Adobe Type Manager Library is a library that Microsoft uses to render PostScript Type 1 fonts inside Windows. A remote attacker can exploit these vulnerabilities to take control of an affected system. Microsoft is aware of limited, targeted attacks exploiting these vulnerabilities in the wild.

There are multiple ways an attacker could exploit the vulnerability, such as convincing a user to open a specially crafted document or viewing it in the Windows Preview pane. Microsoft have provided Mitigation steps that should be implemented, a patch is currently being worked on and will be released in due course.

A number of workaround steps have been provided by Microsoft and CSIRT-IE recommends users review and implement the appropriate workaround as soon as possible. Please see the Security Advisory (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv200006) for the full steps for the relevant workarounds.

3. Mitigation

The workaround steps below have been provided by Microsoft, please see the Security Advisory for the full steps:

- Disable the Preview Pane and Details Pane in Windows Explorer.
- Disable the WebClient service.
- Rename ATMFD.DLL (Please note: ATMFD.DLL is not present in Windows 10 installations starting with Windows 10, version 1709. Newer versions do not have this DLL).

Feedback and Reporting

NCSC-IE wishes to offer whatever assistance it can in relation to this incident and is willing to work with the relevant parties to further understand the current threat. NCSC-IE would also request any feedback in relation to this incident as regards the relevance and accuracy of the information provided.