

令和2年1月15日

内閣サイバーセキュリティセンター
重要インフラグループ

マイクロソフト社製及びMozilla Foundation製ソフトウェアの
更新プログラムについて（注意喚起）

マイクロソフト社製及び Mozilla Foundation 製ソフトウェアのセキュリティ更新プログラムが発表されたので、更新の適用を行ってください。

1. マイクロソフト社製ソフトウェア

1. 1 対象ソフトウェア

Windows、Internet Explorer、Microsoft Office 等の複数のソフトウェア。詳細については参考 URL 参照。

対象ソフトウェアには、リモートでコードが実行される可能性等の複数の「緊急」に分類されている脆弱性が存在。

また、マイクロソフト社の分類では「重要」に分類されているが、米国国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（DHS/CISA）及び米国国家安全保障局が「緊急」と指摘している電子証明書検証に係る脆弱性も存在。

・電子証明書検証に係る脆弱性

Windows 10 等において、Windows CryptoAPI が楕円曲線暗号 (ECC) 証明書を検証処理においてなりすましが可能となるもの。

・Windows リモートデスクトップゲートウェイサーバー及び Windows リモートデスクトップクライアントに係る脆弱性

Windows 7 等において、リモートでのコード実行が可能になるもの。

1. 2 対応

対象ソフトウェアにセキュリティ更新プログラムを適用する。

更新方法等については、参考 URL 参照。

参考 URL

- ・ 2020 年 1 月のセキュリティ更新プログラム (月例) (マイクロソフト社)
<https://msrc-blog.microsoft.com/2020/01/14/202001-security-updates/>
- ・ 2020 年 1 月のセキュリティ更新プログラム (マイクロソフト社)
<https://portal.msrc.microsoft.com/ja-jp/security-guidance/releasenotedetail/2020-Jan>
- ・ CVE-2020-0601 | Windows CryptoAPI Spoofing Vulnerability (マイクロソフト社)
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601>
- ・ Microsoft Windows CryptoAPI fails to properly validate ECC certificate chains
Vulnerability Note VU#849224 (米国 CERT/CC)
<https://kb.cert.org/vuls/id/849224/>
- ・ Alert (AA20-014A)
Critical Vulnerabilities in Microsoft Windows Operating Systems
(米国国土安全保障省サイバーセキュリティ・インフラセキュリティ庁)
<https://kb.cert.org/vuls/id/849224/>
- ・ Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers (米国国家安全保障局)
<https://kb.cert.org/vuls/id/849224/>
- ・ Microsoft 製品の脆弱性対策について (2020 年 1 月) (IPA)
<https://www.ipa.go.jp/security/ciadr/vul/20200115-ms.html>
- ・ 2020 年 1 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (JPCERT/CC)
<https://www.jpCERT.or.jp/at/2020/at200001.html>

2. Mozilla Foundation 製ソフトウェア (Firefox 及び Thunderbird)

2. 1 対象ソフトウェア

- ・ Firefox
- ・ Firefox ESR
- ・ Thunderbird

Mozilla Foundation は昨年 12 月に公開したバージョンに対する脆弱性への対応として、Firefox 72 及び Firefox ESR 68.4 を 1 月 7 日付で公開していたところ。上記ソフトウェアには、実行時コンパイラに新たな脆弱性が存在し、型混乱を引き起こす恐れがあることから、1 月 8 日付で当該脆弱性に対応したバージョン (Firefox 72.0.1 及び Firefox ESR 68.4.1) を公開した。また、1 月 10 日付で Thunderbird についても、当該脆弱性に対応したバージョン (Thunderbird 68.4.1) を公開した。

本脆弱性を悪用した標的型攻撃が確認されており、深刻度が「緊急」とされている。

2. 2 対応

対象ソフトウェアを、最新のバージョンに更新する。
更新方法等については、参考 URL 参照。

参考 URL

- ・ Mozilla Foundation Security Advisory 2020-03
Security Vulnerabilities fixed in Firefox 72.0.1 and Firefox ESR 68.4.1
(Mozilla Foundation)
<https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/#CVE-2019-17026>
- ・ Mozilla Foundation Security Advisory 2020-04
Security Vulnerabilities fixed in Thunderbird 68.4.1
(Mozilla Foundation)
<https://www.mozilla.org/en-US/security/advisories/mfsa2020-04/>
- ・ Mozilla Patches Critical Vulnerability
(米国国土安全保障省サイバーセキュリティ・インフラセキュリティ庁 (DHS/CISA))
<https://www.us-cert.gov/ncas/current-activity/2020/01/08/mozilla-patches-critical-vulnerability>