ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

آسیب پذیری در فونت TrueType

تنظیم کننده:

فروغ فدایی

ویرایش: ۱

شماره سند: V-90/7-6

www.ircert.cc

ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری: V-90/7-6

نام محصول آسیب پذیر: آسیب پذیری در فونت TrueType

نوع سیستم عامل:

کشف توسط: Microsoft

تاریخ کشف:

سطح خطر:

شرح:

مایکروسافت درحال بررسی یک آسیب پذیری در مولفه های مایکروسافت ویندوز است، فونت TrueType در Win32k. مهاجمی که از این آسیب پذیری سوء استفاده می کند، می تواند کدهای دلخواهش را در حالت هسته اصلی اجرا کند. مهاجم می تواند پس از نصب برنامه اطلاعات را ببیند، تغییر دهد یا حذف کند و یا اینکه یک حساب کاربری با دسترسی کامل ایجاد نماید. ما از حملاتی که سعی دارند از این آسیب پذیری گزارش شده استفاده کنند، آگاه هستیم. این آسیب پذیری مربوط به بدافزار Duqu است.

پس از اتمام این تحقیقات، مایکروسافت اقدامات مناسب را جهت کمک به حفاظت مشتریانش انجام خواهد داد. این ممکن است بسته به نیاز مشتری شامل ارائه یک بروز رسانی امنیتی از طریق فرآیند انتشار ماهانه یا ارائه یک بروز رسانی امنیتی خارج از چرخه باشد.

این آسیب پذیری نمی تواند بصورت خودکار از طریق یک ایمیل انتشار یابد بلکه کاربر باید ضمیمه ای را که توسط ایمیل فرستاده شده است، باز نماید.

نرم افزارهای موثر

Affected Software
Windows XP Service Pack 3
Windows XP Professional x64 Edition Service Pack 2
Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Vista Service Pack 2

Windows Vista x64 Edition Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2**
Windows Server 2008 for x64-based Systems Service Pack 2**
Windows Server 2008 for Itanium-based Systems Service Pack 2
Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems and Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1**
Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems Service Pack 1

راه حل ها

از دسترسی به T2EMBED.DLL جلوگیری کنید.

توجه داشته باشید که قبل از استفاده از این راه حل کاربران باید آخرین بروز رسانی های امنیتی مایکروسافت را اعمال کنند. اگر نسبت به بروز رسانی نرم افزارتان مطمئن نیستید، Microsoft Updateرا مشاهده کنید.

همچنین برای این راه حل، دستورات برای ویندوز XP و ویندوز Server 2003 ممکن است فقط در نسخه انگلیسی زبان سیستم عامل کار کند.

در ویندوز XP و Windows Server 2003

- برای سیستم 32-bit دستورات زیر را در administrative command prompt دنبال کنید.

```
Echo y| cacls "%windir%\system32\t2embed.dll" /E /P everyone:N
```

- برای سیستم 64-bit دستورات زیر را در administrative command prompt دنبال کنید.

```
Echo y| cacls "%windir%\system32\t2embed.dll" /E /P everyone:N

Echo y| cacls "%windir%\syswow64\t2embed.dll" /E /P everyone:N
```

در ویندوز Vista و Windows 7 و Windows Server 2008 و Windows Server 2008 R2

- برای سیستم 32-bit دستورات زیر را در administrative command prompt دنبال کنید.

```
Takeown.exe /f "%windir%\system32\t2embed.dll"

Icacls.exe "%windir%\system32\t2embed.dll" /deny *S-1-1-0:(F)
```

- برای سیستم 64-bit دستورات زیر را در administrative command prompt دنبال کنید.

```
Takeown.exe /f "%windir%\system32\t2embed.dll"

Icacls.exe "%windir%\system32\t2embed.dll" /deny *S-1-1-0:(F)

Takeown.exe /f "%windir%\syswow64\t2embed.dll"

Icacls.exe "%windir%\syswow64\t2embed.dll" /deny *S-1-1-0:(F)
```

توصیه های اضافه

با پشتیبانی فنی تماس بگیرید.

از کامپیوتر خود محافظت کنید.

ویندوز خود را بروز نگه دارید.

نرم افزارهای مایکروسافت را بروز نگه دارید.

FAQ

- **هسته ویندوز چیست**؟هسته سیستم عامل است که خدمات در سطح سیستم مانند مدیریت دستگاه، مدیریت حافظه، تخصیص زمان پردازنده به عملیات پردازش و مدیریت رفع خطا را ارائه می دهد.
- **فونت های TrueType چیست**؟این فن آوری از دو بخش تشکیل شده است : فایل خود فونت و برنامه ای که شرح فونت را می خواند و یک تمثال bitmap از فونت را تولید می کند. TrueType یک برنامه کامپیوتری بعنوان بخشی از سیستم عامل است.
- **آسیب پذیری ناشی از چیست**؟زمانیکه یک راننده هسته ویندوز نتواند بدرستی فونت TrueType را بکار برد.

منبع:

http://technet.microsoft.com/en-us/security/advisory/2639658

مرکز آپای دانشگاه شیراز