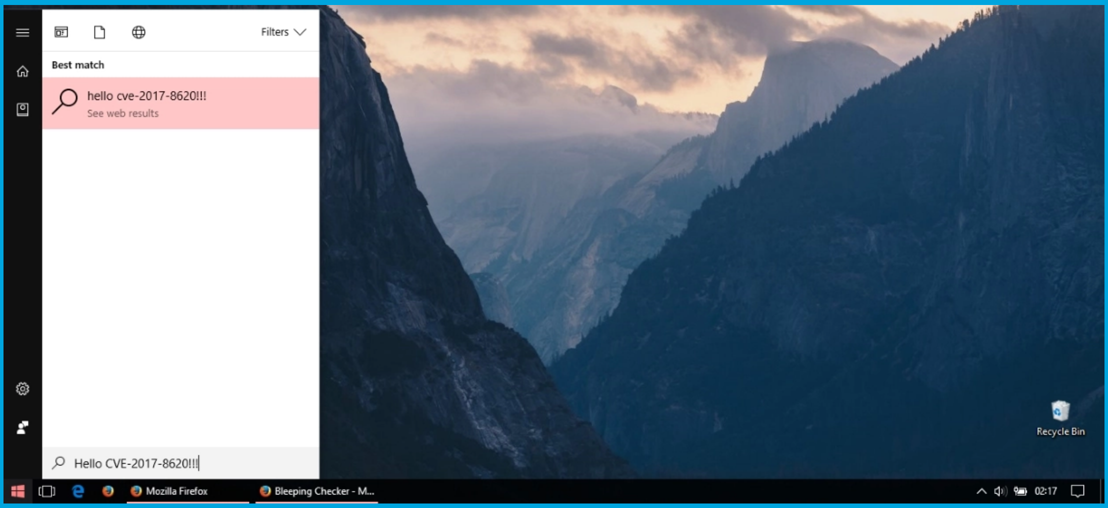
kindred

# Security Newsletter

14 August 2017

# Microsoft Just Fixed a Wormable Bug in Windows Search Affecting All OS Versions



The Microsoft August 2017 Patch Tuesday security patches include fixes for 48 issues, of which 25 are rated critical, but none is as ominous as CVE-2017-8620. This bug is a vulnerability in the Windows Search service and affects all currently supported versions of Windows. The vulnerability allows an attacker to execute code and take over unpatched computers.

To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. An attacker with access to a target computer could exploit this vulnerability to elevate privileges and take control of the computer. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger the vulnerability through an SMB connection and then take control of a target computer."

The danger comes from the vulnerability's potential of being used for self-spreading worms. In addition, Symantec claims that "failed attacks [using CVE-2017-8620] will cause denial of service conditions," leading Windows installations to malfunction or shut down.

In cases where system administrators can't update systems due to incompatibilities and other reasons, Microsoft recommends they disable the WSearch service as a workaround, but this will also disable any search functions on those machines.

Read More

Microsoft Advisory

# Fines for being hacked: If a breach is down to bad security it could cost you millions

Organisations that provide critical national infrastructure services including electricity, water, energy, transport, and healthcare could face fines of £17m or four percent of their global turnover if they fail to protect themselves from cyberattacks.

The plan is being considered by the UK government as it examines how to implement the European Union's Network and Information Systems (NIS) Directive from May 2018. The directive represents the first piece of EU-wide legislation on cybersecurity and provides legal measures in an effort to protect member states and their essential services from cyberattacks.

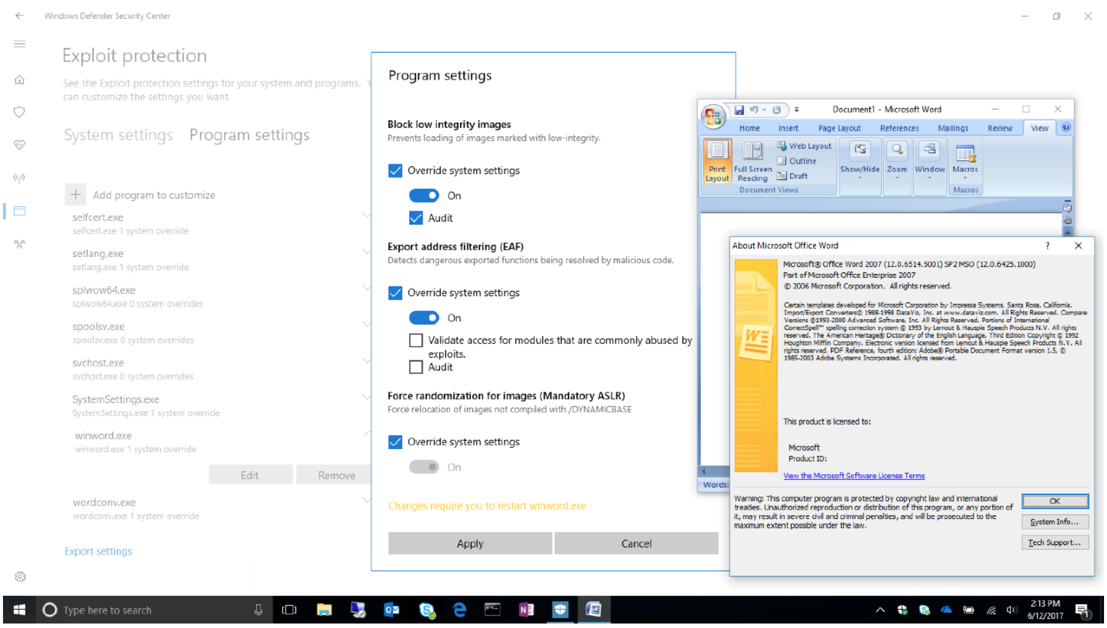
The fines would be a last resort -- and they won't apply to organisations that have put proper cybersecurity protections in place and still suffered a system outage as a result of a cyberattack. At this stage, the government isn't clear about exactly what constitutes taking proper precautions.

NIS is separate from the EU's General Data Protection Regulations -- due to come into force by May 2018 -- which are designed to protect against loss of data, rather than loss of service.

Read More

Even More

# Moving Beyond EMET II – Windows Defender Exploit Guard



Windows Defender Security Center

Exploit protection

See the Exploit protection settings for your system and programs. Y can customize the settings you want.

System settings    Program settings

+ Add program to customize

selfcert.exe
selfcert.exe 1 system override

setlang.exe
setlang.exe 1 system override

splwow64.exe
splwow64.exe 0 system overrides

spoolsv.exe
spoolsv.exe 0 system overrides

svchost.exe
svchost.exe 0 system overrides

SystemSettings.exe
SystemSettings.exe 1 system override

winword.exe
winword.exe 1 system override

wordconv.exe
wordconv.exe 1 system override

Program settings

**Block low integrity images**
Prevents loading of images marked with low-integrity.

☑ Override system settings
● On
☑ Audit

**Export address filtering (EAF)**
Detects dangerous exported functions being resolved by malicious code.

☑ Override system settings
● On
□ Validate access for modules that are commonly abused by exploits.
□ Audit

**Force randomization for images (Mandatory ASLR)**
Force relocation of images not compiled with /DYNAMICBASE

☑ Override system settings
○ On

Changes require you to restart winword.exe

About Microsoft Office Word

Microsoft® Office Word 2007 (12.0.6514.5001) SP2 MSO (12.0.6425.1000)
Part of Microsoft Office Enterprise 2007
© 2006 Microsoft Corporation. All rights reserved.

Certain templates developed for Microsoft Corporation by Impressa Systems, Santa Rosa, California. Import/Export Converters© 1988-1998 DataViz, Inc. at www.dataviz.com. All Rights Reserved. Compare Versions ©1993-2000 Advanced Software, Inc. All Rights Reserved. Portions of International CorrectSpell™ spelling correction system © 1993 by Lernout & Hauspie Speech Products N.V. All rights reserved. The American Heritage® Dictionary of the English Language, Third Edition Copyright © 1992 Houghton Mifflin Company. Electronic version licensed from Lernout & Hauspie Speech Products N.V. All rights reserved. PDF Reference, fourth edition: Adobe® Portable Document Format version 1.5. © 1985-2003 Adobe Systems Incorporated. All rights reserved.

This product is licensed to:

Microsoft
Product ID:

View the Microsoft Software License Terms

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Microsoft recently introduced Windows Defender Exploit Guard (WDEG) which will complete their journey to incorporate all of the security benefits of EMET directly into Windows.

With the Windows 10 Fall Creators Update, you can now audit, configure, and manage Windows system and application exploit mitigations right from the Windows Defender Security Center (WDSC). You do not need to deploy or install Windows Defender Antivirus or any other additional software to take advantage of these settings, and WDEG will be available on every Windows 10 PC running the Fall Creators Update.

To facilitate easy deployment and usage of mitigations without the burden of application compatibility side effects, Microsoft has introduced audit mode support for both EMET legacy app mitigations as well as existing native mitigations provided by Windows.

Windows Defender Exploit Guard includes more than the features integrated from EMET, they will discuss host intrusion prevention capabilities and other WDEG components in a future blog post.

Read More

# A Closer Look at the Ransomware Attacks: Why They Still Work

Ransomware phenomenon continues to dominate the threat landscape and affect important sectors (hospitals, banks, universities, Government, law firms, mobile users) and various organizations equally worldwide.

According to a recent study from Google , ransomware victims have paid more than $25 million in ransoms over the last two years, making the ransomware ecosystem a destructive, yet profitable cyber attack.

All of these cyber threats can target anybody, anywhere and anytime, so remember that awareness and prevention are the best precautions to safeguard your sensitive data.

Read More

No More Ransom

# Source Code Management Tools Affected by Severe Vulnerability

Three of the most popular version control systems (VCSs) used in managing source code projects are vulnerable to a flaw that allows an attacker to run code on a victim's platform, potentially leading to the theft of source code or the hijacking of the underlying machine.

Discovered by Joern Schneeweisz, a security researcher for Recurity Labs, the flaw relies on tricking users into cloning (copying) a source code project via an "ssh://" link. A URL in the form of "ssh://-oProxyCommand=some-command" allows an attacker to execute commands on the computer of the user performing the clone operation.

"While it might be tricky to convince a user to clone a repository with a rather shady looking ssh:// URL, it is possible to create a Git repository that contains a crafted ssh:// submodule URL. When such a repository is cloned recursively, or the submodule is updated, the ssh:// payload will trigger," the researcher added.

Recurity Labs privately disclosed the vulnerability to all affected vendors and waited until all released patches. Yesterday, the company went public with its discovery. Out of all platforms, Schneeweisz says that Subversion is the most vulnerable because the platform doesn't detect HTTP redirects in repository cloning operations.

Read More

Initial disclosure

# NIST Publishes Cybersecurity Workforce Framework

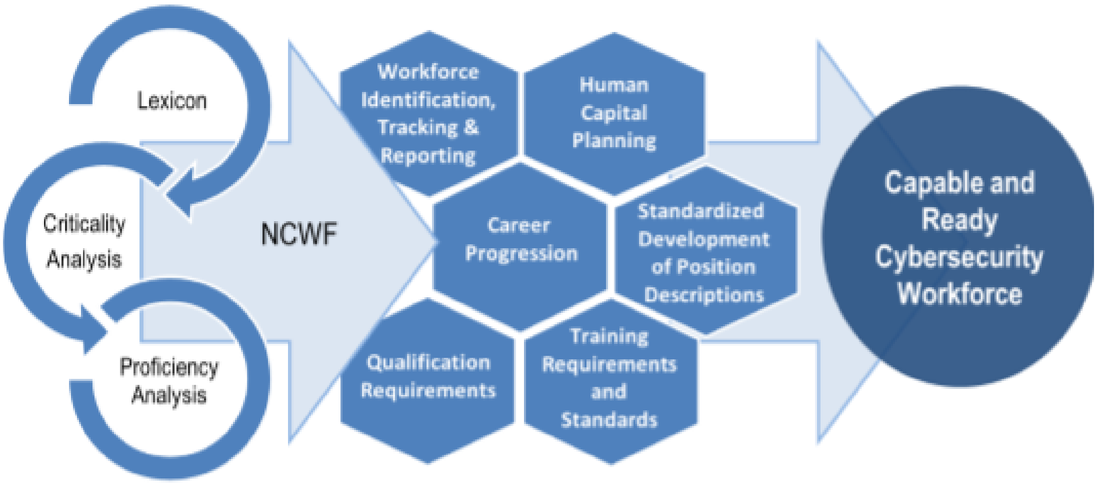

Lexicon
Criticality Analysis
Proficiency Analysis
NCWF
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Cybersecurity Workforce

Figure 1 - Building Blocks for a Capable and Ready Cybersecurity Workforce

The National Institute of Standards and Technology (NIST) has published a cybersecurity workforce framework (PDF) to support organizations' ability to develop and maintain an effective cybersecurity workforce.

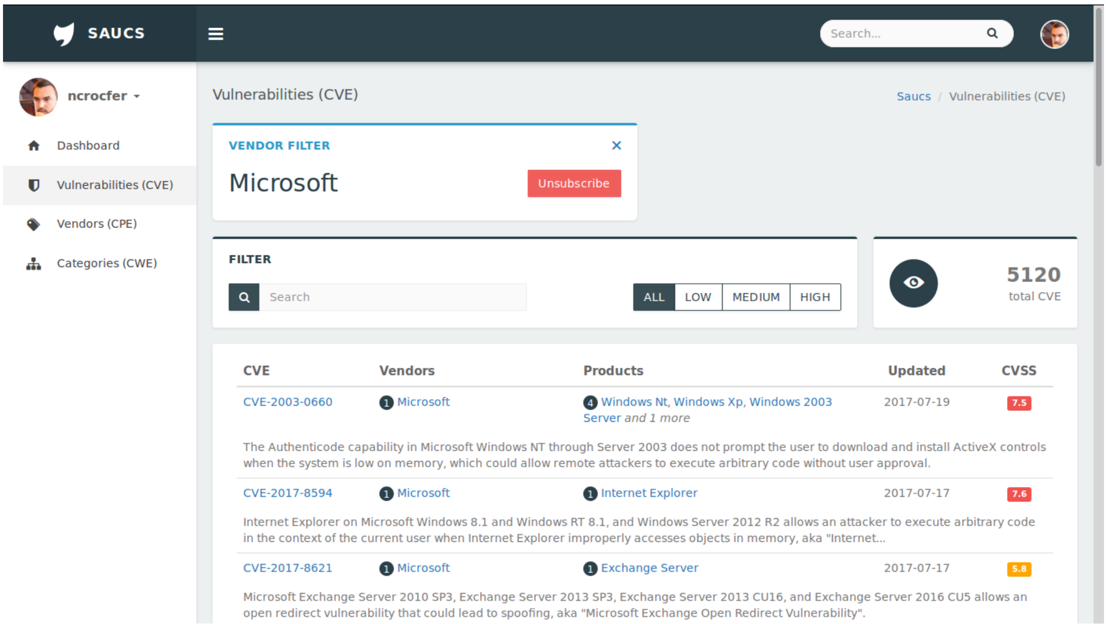
The framework defines roles; necessary knowledge, skills and abilities (KSAs) for those roles; and a common lexicon to clarify communication between cybersecurity educators, trainers/certifiers, employers, and employees. It is intended to help employers develop their existing workforce, and academic institutions prepare the future workforce in a consistent manner.

The NIST framework defines seven primary security workforce categories: Securely Provision; Operate and Maintain; Oversee and Govern; Protect and Defend; Analyze; Collect and Operate; and Investigate. For some, this compartmentalism is a strength; for others, it is a potential concern.

Read More

NIST 800-181

# New Security notification aggregator tool: SAUCS



| CVE | Vendors | Products | Updated | CVSS |
|---|---|---|---|---|
| CVE-2003-0660 | 1 Microsoft | 4 Windows Nt, Windows Xp, Windows 2003 Server *and 1 more* | 2017-07-19 | 7.5 |
| The Authenticode capability in Microsoft Windows NT through Server 2003 does not prompt the user to download and install ActiveX controls when the system is low on memory, which could allow remote attackers to execute arbitrary code without user approval. | | | | |
| CVE-2017-8594 | 1 Microsoft | 1 Internet Explorer | 2017-07-17 | 7.6 |
| Internet Explorer on Microsoft Windows 8.1 and Windows RT 8.1, and Windows Server 2012 R2 allows an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka "Internet... | | | | |
| CVE-2017-8621 | 1 Microsoft | 1 Exchange Server | 2017-07-17 | 5.8 |
| Microsoft Exchange Server 2010 SP3, Exchange Server 2013 SP3, Exchange Server 2013 CU16, and Exchange Server 2016 CU5 allows an open redirect vulnerability that could lead to spoofing, aka "Microsoft Exchange Open Redirect Vulnerability". | | | | |

The operation is simple : you subscribe in 1 click on a vendor (or one of its products), and you receive an alert as soon as they detect a new CVE or an update on it.

We must follow their security updates, which is a day to day job and time consuming. Luckily the CVE standard already exists and provides us this information, but the given data is not easily queryable : we must check all the CVE to see if we are impacted. Saucs goal is to provide this layer and automate everything : our robots check the CVE update list, parse the XML feed and format it. Then you can subscribe to the vendors and products you want, and you receive an email as soon as we detect a new change that will interest you.

As for now, the service is free, we don't know yet what will be the business model. In the meantime, keep in mind that subscribing to this kind of service with a company email can reveal a lot on what services you're using internally.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

## Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.