THE UNIVERSITY OF NEW MEXICO

HLC Accreditation
Evidence Document

Title: Information Security & Privacy Office

Office of Origin: Information Technologies

Description: Information, from their website, on the Information Security & Privacy Office. This office is located with Information Technologies and deals with the privacy and ethical management of data at the university.

Date: 2018

Information Security & Privacy Office

About

The Information Security & Privacy Office (ISPO) is responsible for the development and maintenance of the University's Information Security Program, and providing institution-wide, platform independent professional services.

Information Security Incident Response and Information Security Assessment services guide the University in handling information security and privacy risk. ISPO's services enable the institution to respond to unauthorized disclosure of institutional information, and to identify areas where information assets are not adequately safeguarded.

ISPO seeks to promote a culture that values collaboration, excellence, and integrity.

Mission Statement

The mission of the ISPO is to preserve the confidentiality, integrity, and availability of information assets on systems that collect, store, transmit, and process the information with which The University of New Mexico is entrusted, through people, procedures, and solutions. ISPO provides an Information Security Program and top tier professional services in the interest of supporting the University's overall mission of engaging faculty, students, and staff in its educational, research, and service programs.

Report an Incident

If you suspect that your NetID (i.e. LoboMail account) or a computer have been compromised and you need to know what to do, please see our FAQ

Abuse Report Form

- or -

Help.UNM Self Service

- or -

security@unm.edu

- or -

(505) 277-2497

- or -

UNM EthicsPoint

For more information, visit our Contact Information page

Information Security & Privacy Office

Advisories

The ISPO provides security advisories to the campus community, primarily for IT administrators. Advisories may relate to vulnerabilities that should be patched or to noteworthy security events.

NOTE: These advisories do not indicate that vulnerabilities have been identified on UNM information systems. Vulnerability notifications may be sent privately at the ISPO's discretion.

For more information, please review the ISPO's Vulnerability Management Program Component

January 16, 2019 - Amazon Order Confirmation Scams

Summary:

In response to questions about the recent influx of "Amazon.com Order Confirmation" email schemes, we advise UNM community members who utilize the Lobomail service to be extremely cautious when reviewing email regarding Amazon.com transactions/orders.

These emails appear to contain malicious links that prompt users to download invoices (.doc and .pdf documents) that contain malware.

What UNM is doing:

The Information Security & Privacy Office will continue to monitor the situation, and update the UNM community as needed.

What you need to do:

Delete any unsolicited/unexpected email regarding "Amazon.com Order Confirmation". If you are expecting email from Amazon.com, please refer to their guide to reviewing correspondence from their services.

If you feel your UNM account has been compromised please call UNM's Customer Support Service Desk at (505) 277-5757 or email security@unm.edu.

If you feel you have been the victim of a crime please file a report with UNM PD or visit https://police.unm.edu.

References:

https://www.amazon.com/gp/help/customer/display.html?nodeId=15835501

October 23, 2018 – Phishing/Spoofing Campaigns

Summary:

In response to questions about the recent influx of phishing/spoofing email schemes, we would like to assuage the concerns of the UNM community members who utilize the Lobomail service. In regard to extortion emails, there does not appear to be any evidence of automatic downloads, malware, or other malicious software associated with the email samples provided. *Any credentials (usernames, passwords, etc.) associated with these emails appear to have been the result of high-profile data breaches of parties external to UNM.*

Concerning impersonation emails, all email accounts associated with the impersonation attempts have been hosted by a third-parties external to UNM. As with the extortion emails referenced above, there does not appear to be any indications of account compromises associated with the phishing/spoofing campaigns nor are there any evidence automatic downloads, malware, or other malicious software associated with the email samples provided.

What UNM is doing:

The Information Security & Privacy Office will continue to monitor the situation, and update the UNM community as needed.

What you need to do:

Ensure passwords are not recycled or reused among various accounts/ services. Please be reminded that you should never use your UNM NetID password on non-UNM systems.

If you feel your UNM account has been compromised please call UNM's Customer Support Service Desk at (505) 277-5757 or email security@unm.edu.

If you feel you have been the victim of a crime please file a report with UNM PD or visit https://police.unm.edu.

References:

https://www.ic3.gov/media/2018/180807.aspx

https://www.consumer.gov/articles/imposter-scams

https://www.ic3.gov/crimeschemes.aspx#item-14

September 28, 2018 – Chegg Data Breach

Summary:

In response to questions about the recent data breach affecting more than 40 million registered Chegg user accounts, we would like to assuage the concerns of the UNM community who utilize the Chegg's textbook rental and tutorial services. Chegg has stated that no social security numbers (SSNs) or financial information was obtained in the breach, and the company will be initiating a password reset process for all user accounts. At this time, it appears that only names, email addresses, shipping addresses, Chegg.com usernames, and hashed Chegg.com passwords were disclosed.

What UNM is doing:

The Information Security & Privacy Office will continue to monitor the situation, and update the UNM community as needed.

What you need to do:

Ensure passwords are not recycled or reused among various accounts/ services. Please be reminded that you should never use your UNM NetID password on non-UNM systems.

References:

https://www.zdnet.com/article/chegg-to-reset-passwords-for-40-million-users-after-april-2018-hack/

January 5, 2018 – Meltdown and Spectre Attacks

Summary:

Researchers revealed to chip companies, operating system developers, and cloud computing providers that two major flaws exist within commonly used microprocessors. These flaws, 'Meltdown' and 'Spectre', allow low-privileged users who execute code on your system to read sensitive information from memory via Speculative Execution. Speculative execution is an optimization technique within processors to maximize performance, where a computer system tries to execute instructions even before it is certain that those instructions need execution.

Meltdown applies primarily to Intel processors. The attack takes advantage of a privilege escalation flaw allowing kernel memory access from user space, meaning any secret a computer is protecting (even in the kernel) is available to any user who is able to execute code on a given system.

Spectre applies to AMD, ARM, and Intel processors. It works by tricking processors into executing instructions they should not have been able to, granting access to sensitive information in other applications' memory space.

The difference between the two attacks is Meltdown takes advantage of a specific Intel privilege escalation issue, while Spectre uses the combination of Speculative Execution and Branch Prediction. Both issues can be addressed with software patches. Meltdown, though easier to exploit, is easier to protect against utilizing patches. Spectre may also be protected against with patching, though is a more nuanced process.

What UNM is doing:

UNM is taking steps to test and implement patches as chipset developers and software vendors advise them. Please visit IT Alerts for updates.

What you need to do:

Apply the relevant patches to your devices (Desktop and Laptop Computers, Tablets, Mobile Devices, Embedded Devices, etc.).

References:

https://meltdownattack.com/meltdown.pdf

https://spectreattack.com/spectre.pdf

CVE-2017-5754, CVE-2017-5715, CVE-2017-5753

October 16th, 2017 – Wi-Fi Key Reinstallation Attacks (KRACK)

Summary:

Researchers have discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected Wi-Fi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations. Therefore, any correct implementation of WPA2 is likely affected. To prevent the attack, users must update affected products as soon as security updates become available. Note that if your device supports Wi-Fi, it is most likely affected. During the initial research, it was discovered that Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys, and others, are all affected by some variant of the attacks.

What UNM is doing:

UNM is taking steps to minimize exposure by following our Wi-Fi manufacturer's recommendations and installing a new version of code that includes patches designed to address these issues. Please visit IT Alerts for updates.

What you need to do:

Apply relevent operating system security patches as they are released. Additionally, if you operate a Wi-Fi access point at home, we recommend that you check your router's manufacturer website for firmware updates.

References:

https://www.krackattacks.com/

CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

August 8th, 2017 – Financial Aid Fraud Phone Calls

Summary:

On Tuesday, August 8th, 2017, UNM received reports that UNM students were receiving phone calls soliciting them for apparently fraudulent financial aid offers. While these offers were in the form of a $7,500 educational grant, allegedly from the Department of the Treasury, such offers occur periodically from various sources and in various amounts. The UNM community should be mindful never to provide Personally Identifiable Information (PII) to unsolicited callers. Always navigate to My.UNM and provide any needed information through LoboWeb. If you have questions or believe that you may have received a fraudulent offer, please notify the appropriate UNM office (for example, please notify the UNM Financial Aid Office if you receive seemingly fraudulent financial aid offers).

What UNM is doing:

UNM provides the My.UNM portal for faculty, staff, and students to enter and update any PII needed to enable services that they are requesting. In addition, UNM complies with the law and with law enforcement investigations regarding such matters. In addition, UNM has many resources published to help the UNM community protect themselves from identity theft, and to respond to identity theft when it does occur.

What you need to do:

If you believe an identity theft crime has been committed against you, please contact the UNM Police Department to file a police report. Please forward a copy of that report to the New Mexico State Attorney General and to the Federal Trade Commission (FTC). Please report attempted crimes such as this to the appropriate UNM business office

References:

identitytheft.gov

identityprotection.unm.edu

May 12th, 2017 - WannaCry 2.0 Ransomware

Summary:

On Friday, May 12th, 2017, a large scale ransomware campaign was launched by attackers against various organizations located in over 99 countries. Unlike other forms of ransomeware, WannaCry is primarily distributed to vulnerable systems automatically.

According to US CERT, initial reports indicate attackers are gaining access to enterprise servers either through Remote Desktop Protocol (RDP) compromise or through the exploitation of a critical Windows Server Message Block (SMB) vulnerability.

What UNM is doing:

In an effort to mitigate the risk associated with these attacks, effective immediately, UNM will begin scanning for and blocking vulnerable services related to this attack at the perimeter of the network.

Please be advised, the University began blocking RDP services at the perimeter of the network in August of 2016.

What you need to do:

On March 14th, 2017, Microsoft released a patch to address the vulnerability that WannaCry exploits.

End-users are strongly advised to update all Microsoft software immediately.

System Administrators are strongly advised to install MS17-010 immediately, if they have not already done so.

Reference:

US-CERT Alert TA17-132A

December 29th, 2016 - PHPMailer Vulnerability (CVE-2016-10045)

On Wednesday, December 28, a patch was released for a critical vulnerability in PHPMailer that affects versions prior to 5.2.20. Please be advised there are active exploits for this vulnerability which allow an unauthenticated adversary to perform remote code execution. While some systems may not be vulnerable, it is strongly advised all system administrators patch and test their systems according to their procedures.

For details about PHPMailer vulnerabilities, please see:

https://github.com/PHPMailer/PHPMailer/blob/master/SECURITY.md

December 24th, 2016 - Lynda.com Data Breach

In response to questions about the recent data breach affecting more than 9.5 million Lynda.com user accounts, we would like to assuage the concerns of the UNM community who utilize the service via the University's Lynda.com gateway (Lynda.UNM). The passwords of UNM users who access the online learning service via Lynda.UNM have not been compromised. At this time, it appears that only user course data and user-provided contact information may have been disclosed.

The Information Security & Privacy Office will continue to monitor the situation, and update the UNM community as needed.

Please see the following article for more information:
http://www.forbes.com/sites/leemathews/2016/12/19/9-5-million-users-warned-after-lynda-com-breach/

October 21st, 2016 - Linux kernel vulnerability (CVE-2016-5195)

On Thursday, October 20, a patch was released for a critical vulnerability (CVE-2016-5195) in the Linux kernel. Please be advised there are active exploits for this vulnerability which allow an adversary to escalate privileges. While some systems may not be vulnerable, it is strongly advised all system administrators patch and test their Linux systems according to their procedures. Please reference the following information:

For details about the vulnerability, please see: access.redhat.com/security/cve/CVE-2016-5195

For details about the kernel patch, please see: lkml.org/lkml/2016/10/19/860

For an article describing potential impact of the vulnerability, please see:
arstechnica.com/security/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/

September 12th, 2016 - Dropbox Data Breach

In response to the breach of more than 68 million Dropbox user accounts and passwords, UNM is reiterating the need for the more than 3,400 Dropbox users who sign in to Dropbox using their NetID to log in as soon as possible, at which point those users will be directed to change their Dropbox password.

Please be reminded that you should never use your UNM NetID password on non-UNM systems. Additionally, Dropbox is not a UNM approved vendor/ application for collecting, storing, transmitting or processing any data for which UNM is entrusted.

August 8th, 2016 - Suspention of RDP-based services

Yesterday afternoon, UNM IT detected a pattern of abnormal network traffic.

The pattern of traffic appears to be a distributed attack against NetID accounts using lists of commonly-used passwords. This attack has resulted in NetID accounts being locked out for extended periods during the day, and could result in accounts being compromised.

The attack used the Remote Desktop Protocol (RDP) which can be used as a tool for remotely connecting to servers, as well as to workstations. Using RDP by itself, without additional safeguards or controls, is not a best practice method for remotely accessing servers or workstations, as it directly exposes those hosts to such attacks.

To help mitigate these attacks and to prevent users from being locked out of all Windows Active Directory (AD) based services (such as LoboMail, Office365, and AD authenticated workstations), effectively immediately, UNM IT will begin blocking RDP services at the perimeter of the UNM network while we research a more sustainable approach.

April 13th, 2016 - Badlock Windows & Samba Bug - Multiple CVEs

The UNM Information and Privacy Office (ISPO) wants to alert you that on April 12, 2016, both Microsoft and Samba issued patches for vulnerabilities in the file-sharing protocol originally called Server Message Block (SMB) but now called Common Internet File System (CIFS). The vulnerability dubbed Badlock allows an escalation of privileges by intercepting some types of Windows logons through a Man in the Middle (MiTM) attack.

Microsoft released patch MS16-0471 during yesterday's Patch Tuesday 4/12/2016 for CVE-2016-0128. Samba also released Samba 4.4.2, 4.3.8, and 4.2.11 Security Releases2 for CVE-20162118.

Solution:
Due to the emerging risks outlined above, the UNM ISPO strongly recommends that affected users apply the available updates to affected systems that require SMB/CIFS. We recommend disabling the SMB/CIFS protocols from computers where it is not required. At a minimum, keeping installed SMB/CIFS protocols current with security patches.

References:

- https://technet.microsoft.com/library/security/ms16-047
- https://www.samba.org/samba/security/CVE-2016-2118.html

April 13th, 2016 - Critical Adobe Flash Vulnerability CVE-2016-1019

The UNM Information and Privacy Office wants to alert you that on April 7, 2016, Adobe patched several Flash Player vulnerabilities, including a critical vulnerability that could lead to remote code execution on a target computer. Adobe issued this patch as an out-of-cycle emergency update as they believe one of the vulnerabilities (CVE-2016-1019) is being actively exploited1. Over 20 total vulnerabilities in Flash Player were addressed in this update from Adobe.

The disclosed vulnerabilities would allow an attacker to remotely crash the targeted computer or potentially execute arbitrary code on that device. This vulnerability impacts versions of Adobe Flash Player prior to the newly-released v21.0.0.213 on Windows, Mac OS X, Chrome OS, and v11.2.202.616 on Linux operating systems.

Adobe is aware of current attacks, using the Magnitude Exploit Kit, to actively target vulnerable versions of Flash Player running on Windows 10 and earlier operating systems2. The Magnitude Exploit Kit opens the door to a Locky Ransomware injection that abuses macros in document files to encrypt user files on the infected computers.

Solution:
Due to the emerging risks outlined above, we strongly recommend that affected users apply the available update to affected systems that have Flash installed. We recommend uninstalling Flash from computers where possible, and at a minimum, keeping installed plugins current with security patches.

The new version of Flash Player is v21.0.0.213 on most platforms and is v11.2.202.616 on Linux.

References:
https://helpx.adobe.com/security/products/flash-player/apsa16-01.html

https://helpx.adobe.com/security/products/flash-player/apsb16-10.html

March 1st, 2016 - Please Implement OpenSSL patches or otherwise disable SSLv2

OpenSSL has published a security advisory requesting that administrators install patches:

- OpenSSL 1.0.2g for 1.0.2 users
- OpenSSL 1.0.1s for 1.0.1 users
- Or otherwise disable SSLv2

The Information Security & Privacy Office is requesting that all versions of SSL be disabled and replaced by TLS 1.1 or above. The ISPO periodically scans the UNM computing network to ensure that vulnerabilities such as this are remediated. For questions about remediation, please consult your vendor documentation. For questions regarding remediation validation, please reply from this thread but to the address security@unm.edu or open a Service Request in Help.UNM.

The full advisory is pasted verbatim below the signature and can be viewed at:
https://www.openssl.org/news/secadv/20160301.txt

The United States Computer Emergency Readiness Team (US-CERT) issued their own alert on 3/1/2016: https://www.us-cert.gov/ncas/current-activity/2016/03/01/OpenSSL-Releases-Security-Advisory

July 8th, 2016 - Zero-Day Adobe Flash Player Vulnerability

Recently, awareness of a zero-day vulnerability for Adobe Flash Player surfaced. Dubbed "the most beautiful Flash bug for the last four years"
by the hacker group who's leaked documentation lead to the publicity of the vulnerability.

Impact:
Sources [1] indicate that this vulnerability is actively being exploited in the wild. Successful exploitation can result in remote code execution.

Platforms Affected:
Adobe states that all previously released versions of Adobe Flash are affected, including those bundled with Adobe AIR.

Mitigation:
Immediately update Adobe Flash Player to 18.0.0.203.
Immediately update AIR Desktop Runtime to 18.0.0.180.
More version information can be found here. [2]

Recommendation:
To help mitigate potential future threats, enable Click-to-Play for the Adobe Flash Player add-on.

Further Reading:
+ Adobe's Player Download Center site [3] Helpful hints for managing the
+ Adobe Flash add-on [4] Enabling 'Click-to-Play' for the Adobe Flash
+ Player add-on [5] Details regarding the latest vulnerability [6]

References:
[1] http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/
[2] http://www.adobe.com/software/flash/about/
[3] https://get.adobe.com/flashplayer/
[4]
http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html
[5] http://www.howtogeek.com/188059/how-to-enable-click-to-play-plugins-in-every-web-browser/
[6] http://labs.bromium.com/2015/07/07/adobe-flash-zero-day-vulnerability-exposed-to-public/

November 18th, 2014 - Microsoft Kerberos Key Distribution Center Patch

Earlier today Microsoft released a critical out-of-band patch for a vulnerability in the Kerberos Key Distribution Center (KDC). Kerberos is the mechanism used to exchange the cryptography keys in Active Directory authentication (AD) systems. The vulnerability allows a person with valid AD credentials to elevate their privileges to those of a domain administrator. This affects all currently supported Microsoft operating systems in Active Directory domains. Microsoft strongly encourages customers to apply this update as soon as possible. Information Technologies is currently working to test, patch, and verify core UNM enterprise systems.

Full list of affected Microsoft products use search engine terms "Microsoft Security Bulletin MS16-068"

References:
blogs.technet.com/b/msrc/archive/2014/11/18/out-of-band-release-for-security-bulletin-ms14-068.aspx

CVE-2014-6324

October 17th, 2014 - POODLE, Sandworm

This week, two new significant security vulnerabilities were discovered. One is an SSL version 3.0 vulnerability called Poodle and is a cross-platform (PC and Mac) vulnerability. The other vulnerability is called Sandworm and it affects all currently-supported versions of Windows. The UNM IT Security Team is addressing this now and recommends using a current fully patched operating system and browser.

The **Poodle** vulnerability is serous because most web servers and browsers still support SSL version 3, even though the more robust TLS encryption is replacing it. Many systems still support SSL v3 for backward compatibility with older browsers like Internet Explorer 6.

The **Sandworm** vulnerability affects all current Windows products up to and including Windows 8.1 and Server 2012. Sandworm allows remote code execution on vulnerable computers by exploiting a flaw in the way Windows handles Object Linking and Embedding (OLE). Attackers can embed OLE files from external sources to download and install malware on to the target's computer. Microsoft released a patch (MS14-060) for Sandworm earlier this week as part of its "Patch Tuesday" updates. Please ensure this is installed.

The ISPO is ensuring all UNM hardware and software is appropriately updated to protect the community.

October 14th, 2014 - Dropbox username and password leak

There are unconfirmed reports that up to 7 million Dropbox usernames and passwords have been leaked. Dropbox denies any of its services have been hacked and states other "third party services" are responsible for the leak.

So far there have been 4 small batches of usernames and passwords posted in plain text on Pastebin and the user responsible claims to have 7 million accounts. This person is asking for BitCoin donations to continuing posting batches of account information. Some of the posted credentials have been confirmed as active and legitimate, allowing login to Dropbox.

UNM does not condone the use of Dropbox for any UNM data. The Information Security team recommends that Dropbox users immediately change their Dropbox password and use a username-password combination that is unique to only Dropbox. Multifactor authentication is an additional layer of protection and is available for Dropbox accounts.

We will continue to monitor this issue for additional developments.

September 29th, 2014 - BASH vulnerability (Shellshock) Update

Late last week a statement was released by IT regarding the recently disclosed BASH vulnerability known as Shellshock. While that information was meant for the general campus community, here is a follow-up for a more technical audience.

This is a fact based description of the vulnerability:

> Search engine terms "US-CERT Alert (TA14-268A)" or https://www.us-cert.gov/ncas/alerts/TA14-268A

Here is a good list of vendors and products and whether they are affected by the BASH vulnerability:

> Search engine terms "Vulnerability Note VU#252743" or http://www.kb.cert.org/vuls/id/252743

This vulnerability is being actively targeted and exploited in the wild.

The UNM Information Security & Privacy Office is continuing to assess UNM's exposure to this bug.

September 26th, 2014 - Shellshock Update

As you may have heard, there is a new, potentially widespread, vulnerability affecting computers, but more commonly servers, dubbed Shellshock.

What UNM is doing
The Information Technology department is aware of the Shellshock bug and has been actively scanning and updating our servers, where appropriate, to address any vulnerabilities. Many UNM services, including Lobomail and MyUNM, have not been affected. While the threat is serious, the impact is not yet known. However, UNM IT already has multiple layers of protection in place to prevent the exploitation of these types of vulnerabilities.

What you should do
Don't panic. Not all systems are vulnerable, and many websites are already installing patches on their systems.

The best defense against vulnerabilities like this one would be to adhere to these security best practices:

1. Routinely change passwords.
2. Using different passwords for different websites, especially your financial websites.
3. Use your UNM NetID and password combo only for UNM sites and business. Do not use this combination of username and password on 3rd party sites, trusted or not.
4. Use multifactor authentication when possible. Many sites, like banks, credit unions and even Facebook, now offer this service but do not require it.
5. Expect new email phishing and social engineering campaigns to take advantage of this wave of fear many users may now have in the wake of this announcement.

To find out more about this bug, visit https://www.us-cert.gov/ncas/alerts/TA14-268A

For a comprehensive, updated list of consumer sites affected by Shellshock, please visit http://www.pcworld.com/article/2687857/bigger-than-heartbleed-shellshock-flaw-leaves-os-x-linux-more-open-to-attack.html.

The UNM Security & Privacy Office continues to ensure the University's data is protected and we will keep you updated.

August 7th, 2014 - US-CERT: OpenSSL Patches Nine Vulnerabilities

OpenSSL has released updates patching nine vulnerabilities, some of which may allow an attacker to cause a Denial of Service (DoS) condition or force the client to revert to a less secure Transport Layer Security (TLS) 1.0 protocol. The following updates are available:

-OpenSSL 0.9.8 users should upgrade to 0.9.8zb

- OpenSSL 1.0.0 users should upgrade to 1.0.0n

- OpenSSL 1.0.1 users should upgrade to 1.0.1i

US-CERT recommends users and administrators review the OpenSSL Security Advisory for additional information and apply the necessary updates.

May 28th, 2014 - Security Vulnerability in TrueCrypt

Please see the article in the link below regarding today's announcement by TrueCrypt of major vulnerabilities in the TrueCrypt product.

http://www.theregister.co.uk/2014/05/28/truecrypt_hack/

The ISPO does not recommend nor support this product, but we are aware that some departments do, and as such, should be informed about the major security risks associated with the use of this product.

May 1st, 2014 - IE Browser Patch Being Tested

As the news or social media may have informed you, there is a significant vulnerability in Microsoft Internet Explorer (IE), versions 6, 7, 8, 9, 10 & 11. Microsoft has not indicated whether or not it would issue a patch before the next scheduled patch day.

This vulnerability rates as a 10/10, the highest risk to consumer data and exists in the browser, not the sites you visit; however, the code that exploits the browser vulnerability may be present on sites you visit. The rating and the methodology to determine this rating are both viewable at NIST.gov (linked below).

To find out more about this bug, please visit:
www.kb.cert.org/vuls/id/222929

web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1776

www.us-cert.gov/ncas/current-activity/2014/04/28/Microsoft-Internet-Explorer-Use-After-Free-Vulnerability-Being

What you should do:
First of all, don't panic. You must visit a compromised web page in order to have malicious code related to this bulletin execute on your machine.

Unfortunately, if this zero-day vulnerability is exploited on your machine, a complete compromise is possible. This vulnerability is currently being exploited across the Internet.

Based on recommendations from the Department of Homeland Security and from other information security news, UNM IT recommends using an alternative browser such as Mozilla Firefox or Google Chrome.

Please seek your local IT support for assistance with installing an alternative browser.

Expect new email phishing and social engineering campaigns to take advantage of this vulnerability.

What UNM is doing:
After careful review, UNM Information Technologies has implemented filters on the UNM Main Campus network to help detect and mitigate any exploitation of the vulnerability. IT is diligently reviewing UNM systems to ensure that they are not compromised, but because this vulnerability exists in IE on user machines and not on servers (such as the recent Heartbleed event), there are few other actions UNM IT can take to mitigate risk to end user data.

We continue to ensure the University's data is protected and we will keep the community updated.

April 11th, 2014 - Heartbleed Update Day 5

Here is another update for the Heartbleed bug. There is good news, bad news and really bad news with a glimmer of hope.

The Bad News: 2 vulnerable SSL certificates discovered affected the Juniper VPN concentrator, vpn.unm.edu. This device is now updated and the new certificates are in place. This means anyone with VPN access will be required to change their NetID password even if the password was changed in the last 5 days. Communications to those users will be sent in a separate email. Even if you do not use the VPN, it is strongly recommended that any users with elevated privileges; systems administrators, departmental IT support personnel, etc. change passwords too.

The Really Bad News: As many information security researchers feared, there is strong evidence that this vulnerability in SSL was known by sophisticated malicious hackers since November 2013, possibly earlier. They are probably at the intelligence agency and nation-state level; likely the same people that brought us APT1. The glimmer of hope is most of that activity appears to have targeted the same level of systems, not consumers and other end users.

The Good news: Information Security, working with multiple teams at Information Technologies, have identified some systems that were affected by the Heartbleed bug. Our initial priority were core IT services. Those identified have been updated and new certificates installed. We also checked all the SSL certificates issued through IT Software Distribution and 9 of 163 were vulnerable. That percentage, 5.5%, is pretty consistent with the number of systems we are discovering to be vulnerable to Heartbleed. We have contacted the systems administrators with the vulnerable certificates to get them revoked and reissued.

Now that we are moving out of the identification, containment, and remediation stages of this incident, constant vigilance is essential. The next phase for us is continued monitoring. Information Security and IT: Networking will continue to monitor network traffic for the specific traffic patterns of Heartbleed. When discovered, we will notify IT personnel in the affected areas.

Attached is a list of SSL certificates we have tested and verified are not currently affected by Heartbleed. This list is not all inclusive, it is what we have tested so far. Further testing will be an ongoing process.

Report an Incident

If you suspect that your NetID (i.e. LoboMail account) or a computer have been compromised and you need to know what to do, please see our FAQ

Abuse Report Form

- or -

Help.UNM Self Service

- or -

security@unm.edu

- or -

(505) 277-2497

- or -

UNM EthicsPoint

For more information, visit our Contact Information page

Information Security & Privacy Office

FAQ

Click questions to expand answers.

ISPO Services

How do I contact or request service from the ISPO?

How do I submit a request to establish or modify a firewall rule?

How do I request an information security review for my purchasing request?

How do I request an information security review for a contract or legal clause?

Malware & Hacking

What do I do if I suspect that my UNM-owned computing asset has been compromised?

What do I do if I suspect my personal computing asset has been compromised?

NetID Issues

My account (NetID) was locked by ISPO, who do I contact to have my account unlocked?

What do I do if I suspect that my account (NetID) is compromised?

Email Issues

What do I do when I get spam email?

What is phishing email, how is it different from "spam", and what do I do when I get it?

You asked me to send an email message as an attachment, how do I do that?

Other

I didn't find the answer I was looking for, who do I contact for more information?

Report an Incident

If you suspect that your NetID (i.e. LoboMail account) or a computer have been compromised and you need to know what to do, please see our FAQ

Abuse Report Form

- or -

Help.UNM Self Service

- or -

security@unm.edu

- or -

(505) 277-2497

- or -

UNM EthicsPoint

For more information, visit our Contact Information page

Albuquerque, NM 87131, (505) 277-0111
New Mexico's Flagship University