Protect your Lab Identity with Multi Factor Authentication

We’ve all heard the stories about major data breaches at some of the largest online businesses. 3 billion Yahoo customers had their usernames and passwords compromised leaving those users vulnerable to hackers. Target was breached in 2013, exposing the information of 41 million customers.

A strong password is no longer enough to protect you and your data. Multi Factor Authentication (MFA) provides a second layer of security beyond your username and password. Think of it this way: your username and password are “something you know.” MFA requires both “something you know” and “something you have.” At Berkeley Lab, the “something you have” is a physical token that will generate a unique one-time password (OTP). Under MFA, a hacker who has your credentials still can’t access your account, because they lack “the something you have.”

Berkeley Lab has implemented MFA protection for your Berkeley Lab Identity. As a computing best practice and to help protect you against credential theft, you can choose to add MFA protection for your Single-Sign-On (SSO) logins, such as Gmail, Google Calendar, Google Team Drive, LETS, HRIS, etc.

To adopt MFA for your account, follow these simple steps:

1. Update your Notification Information at https://password.lbl.gov
2. Set up Google Authenticator
3. Get a YubiKey token by either
   a. submitting a ticket to help@lbl.gov
   -or-
   b. attending an IT workshop in your area

Detailed instructions are available in the Multi Factor Authentication Instructions page.

For additional help, create a ticket by emailing help@lbl.gov.

Related Sites

- Multi Factor Authentication
- Multi Factor Authentication Instructions
- Multi Factor Authentication Token Management
- YubiKey for Multi Factor Authentication
- Google Authenticator for Multi Factor Authentication
- Resync Your YubiKey

Endless Reboot Loop Due to macOS High Sierra Update

Problem

The IT User Support Group has had several calls from customers this morning regarding the endless reboot loop of their
system after installing the latest High Sierra macOS update. Error message is,

“The path /System/Installation/Packages/OSInstall.mpkg appears to be missing or damaged. Quit the installer to restart your computer and try again.”

The system then enters an endless reboot and does not let you log into the computer.

Solution

1. Ensure you have a backup of your computer
2. Turn off your computer
3. Holding down the “Option” key, reboot your computer
4. From the boot menu provided, select your hard drive, i.e. Macintosh HD or the name of your hard drive
5. Log into your computer
7. Install the update
8. Reboot your computer

If you have any questions, please feel free to contact IT at help@lbl.gov or click on the link below.

REQUEST HELP

Backup Solution

Go to the software download page and request a Druva inSync backup account. For more information see, Backups.

Why Use a Password Manager Like LastPass?

Generating, remembering and maintaining unique passwords is challenging and nearly impossible today. As the number of mandatory passwords, password length, and password complexity increases, it becomes harder to remember them without relying on risky alternatives such as writing passwords down or reusing passwords for more than one application. Reuse of a password is one of the biggest security vulnerabilities today. Given the recent high profile breaches of company’s user data, if you reuse a password on more than one site you are at risk for all your other sites. Do you know where you reuse your password?

The solution to address this problem is a password manager. Berkeley Lab has now adopted LastPass as an enterprise password manager and you can download it for free from our software download page, https://software.lbl.gov/swSoftwareDetails.php?applicationID=191.

LastPass resides in your browser and helps you store, manage, and automatically provide account name/password information to web-based applications. As you enter your credentials, LastPass automatically stores it in your safe, encrypted vault. When you are prompted to provide your credentials, LastPass will automatically identify the correct username and password to enter. Access to your vault is through your “master” password. Your master password is the only password you need to remember.

LastPass has additional features:

- The ability to sync your vault across any device on any platform at any time
- The ability to utilize multi-factor authentication
- The ability to share logins and passwords safely across an organization
- The ability to run a security check against your password vault to determine where there are duplicates and weaknesses

Don’t wait to get compromised, get your copy of LastPass today.

Related News

- Berkeley Lab IT LastPass website, https://commons.lbl.gov/display/itfaq/LastPass
- Official LastPass Blog - What LastPass users Need to Know about Meltdown and Spectre
High Sierra - Upgrade or Not to Upgrade

IT always cautions users to never upgrade your operating system until you do the following:

- Ensure you have a full backup of your system just in case you need to roll back
- Ensure all your current versions of software and peripherals are compatible with the new operating system, see https://roaringapps.com/ for compatibility tables

For Operations Mac users, IT blocked the upgrade to High Sierra due to incompatibilities with Office 2011, Office 2016 (v15.34 and below), Spirion (formerly known as Identity Finder) and Sophos. IT has now confirmed that Office 2016 v15.35 and higher, Spirion and Sophos are now compatible with macOS High Sierra. IT has now:

- Allowed the installation of macOS High Sierra to be installed on all systems with Office 2016 version 15.35 and higher
- Has blocked macOS High Sierra to be installed on systems with Office 2011

IT recommends that users of systems running compatible versions of these applications upgrade to High Sierra. If, following the upgrade, an application is not behaving as expected, users should reinstall the affected application and repeat the testing. While a reinstall of the your software should usually address the issue, problems may persist. If this does not resolve the problem, please open a help ticket via the link below.

REQUEST HELP

This project was possible because IT identified affected systems with BigFix and Casper. To get BigFix for your computer, please visit software.lbl.gov.

Related News

- Microsoft Office support for macOS 10.13 High Sierra
- High Sierra leaves Microsoft Office for Mac 1011 behind, 2016 edition needs updating

MacKeeper Introduces More Problems Than It Is Worth

MacKeeper is a well-known utility suite for macOS, which is typically installed by users looking to improve the performance of their system. MacKeeper is known to use aggressive marketing techniques, and has a very poor track record in terms of security, and in its ability to perform as advertised. Further, MacKeeper has been known to destabilize a Mac, undermining its stated purpose.

MacKeeper is increasingly seen as malware because of its pervasive pop up ads and can even be considered spyware. Sophos reported Mackeeper as 2017's most prolific potentially unwanted program on the Mac. Most alarmingly, Mackeeper has a very poor record on security. For example:

- In 2015 MacKeeper had a major security breach of its customer accounts
- Also in 2015, MacKeeper had a major security flaw which gave attackers full access to control a user’s Mac

With the help of BigFix, we have identified users with MacKeeper on their systems. We will be reaching out to those Lab employees to let them know that we wish to remove MacKeeper from their systems for security reasons. Communication will occur prior to any action.

If you have any questions, please feel free to contact IT at help@lbl.gov or click on the link below.

REQUEST HELP

This project was possible because IT identified affected systems with BigFix. To get BigFix for your computer, please visit software.lbl.gov.
How BigFix Can Help You

Do you want to:

1. Increase your computer security, and reduce the effort needed to keep it that way?
2. Inventory and report potential computer software and hardware issues?
3. Help find and track your computer assets?

BigFix can help! In fact, Berkeley Lab IT has BigFix deployed on over 4000 Windows, Mac and Linux systems across the Lab. We recommend that all employees install BigFix on all desktop and laptop systems at the Lab. To get started now, install BigFix from software.lbl.gov.

The single most important thing you can do to protect your system is to keep the operating system and all applications up to date with the latest patches. Hackers target computer running obsolete operating systems and applications, which have well-known and easily-attacked vulnerabilities. For example, if you are running an older web browser, email program, image viewer, instant messaging, or even media player, your system is susceptible to infection with no action on your part other than viewing a malicious site. By installing BigFix, you can be sure that your system will always be running the latest version of the operating system and the most commonly compromised applications. For more information, see https://commons.lbl.gov/display/itfaq/Patch+Management+Services.

BigFix is also used to detect and report on common issues with your system, including low disk space, vulnerable programs, and even failing hard drives. IT User Support can then proactively help you address these problems before disaster strikes! For example,

- In October 2017, the popular system utility CCleaner was hacked, and malware was embedded into the newest updates. We were able to identify who had CCleaner installed, notify users of the vulnerability, and help them clean up their systems. For details, see https://commons.lbl.gov/display/itfaq/2017/10/12/CCleaner+Hacked.
- In October 2017 Microsoft released a Windows patch that could cause a computer to fail boot. IT User Support was able to identify these systems, and worked with the users to ensure that reboots were done in a way that wouldn’t impact their work.

BigFix is also being used in the Lab’s current Wall-to-Wall inventory campaign! Any DOE-barcoded system running BigFix and on the LBL network can be automatically checked in to SunFlower, saving your property rep from having to manually scan the barcode. This pilot program is currently under development by the IT and CFO divisions.

For these and many other reasons, we encourage you to install BigFix on your computer systems. BigFix is available from software.lbl.gov.

If you want further information regarding BigFix or need help installing BigFix, enter a help ticket by clicking on the Request Help link below.

REQUEST HELP

Apple MacOS High Sierra Security Bug

Problem
As reported yesterday, there's a major security flaw in Apple's newest operating system, High Sierra. The bug allows anyone to gain complete administrative access to the computer when using "root" as the username with a blank password. Berkeley Lab's Cybersecurity team has released this information, Apple OSX High Sierra 10.13 authentication bug.

Solution


BigFix Deployed Apple Update

As of this 11/30/2017 AM, we had some users who had not installed the Apple security update. BigFix discovered these systems and installed the update automatically.

Password Requirements Have Changed

Cyber Security recently changed Berkeley Lab Identity password requirements. The changes included:

- Your passphrase must be at least 14 characters
- Your passphrase must pass a strength check that disallows repeated / sequential characters, keyboard patterns, and other trivial passwords
- Your passphrase must be changed every 12 months, rather than 6 months

For more information see Password Requirements - 2017 Update.

Windows 10 Patch Causes Computer Boot Failure

Problem

Microsoft recently announced that Windows devices may fail to boot after installing Windows 10 Updates that were released on October 10 2017. This is the result of a problem on Microsoft's end in publishing the updates with IDs KB4041676 and KB4041691. Microsoft has since revoked these updates, and has provided solutions for affected systems, as detailed below. Functional versions of these patches have since been released. It is estimated that as many as 265 Windows 10 systems running at Berkeley Lab may be impacted. These systems were identified because they have BigFix installed.

If you received an email from IT User Support about this issue, then your system has the potential to be affected. Even if your system appears to be working fine, there is a possibility that your system will fail to boot upon your next restart.

Note that applying the Microsoft-recommended fix for this issue will require advanced Windows skills, and is best done by an IT professional. You can either apply one of the solutions listed below or contact the IT Help Desk by clicking here to email help@lbl.gov.

While this issue should not cause any loss of data, IT User Support reminds all users that all computers should be backed up, and recommends Druva inSync for this purpose.

Solution
Scenario: Windows 10 devices that downloaded the October 10 KB4041676 or KB4041691 update with publishing issues and have NOT YET BEEN REBOOTED


Scenario: Windows 10 devices that downloaded the October 10 KB4041676 or KB4041691 update with publishing issues and are unable to boot into Windows.


This project was possible because IT identified affected systems with BigFix. To get BigFix for your computer, please visit software.lbl.gov.

Why Chrome OS?

See how the IT User Support Department is trying to stretch dollars to support science, see our story at Chrome OS.

CCleaner Hacked

Problem

Some CCleaner installers were found to have third party malware embedded. Though CCleaner fixed their installers quickly, some of users downloaded and unknowingly installed malware. A project in IT User Support was initiated to identify these systems and notify users that their computers could be compromised. We requested removal of the software and a complete Sophos scan to be run to confirm removal of the infected software. We are continuing to monitor systems for potential threat using BigFix.

Solution

IT User Support advised staff to do the following:

1. Uninstall CCleaner
2. Run a Sophos scan. If you don’t have Sophos installed, please download for our software download page (https://software.lbl.gov)

Related news

Please note as a part of this investigation, we discovered that the free version of CCleaner cannot legally be installed on Laboratory computers. The IT User Support will be issuing a BigFix offer to remove this software at user convenience. If you don't have BigFix installed on your system please see our IT Software Download Page at https://software.lbl.gov.

This project was possible because IT identified affected systems with BigFix. To get BigFix for your computer, please visit software.lbl.gov.
Acrobat End of Life (EOL)

As of October 16, 2017, Adobe will no longer be supporting and providing security patches for Acrobat 11 and all previous versions. If a security vulnerability is identified after October 16, 2017, Cybersecurity may block you from our network unless you do one of the following:

Option 1: Upgrade to Adobe Acrobat DC
Adobe has now moved to a cloud-based subscription model of Adobe Acrobat, called Adobe Acrobat DC. The current cost for Adobe Acrobat DC from the Lab’s software site is $160.00 per year. This is an annual subscription with the potential to increase by 3 to 5% annually.

There is no direct upgrade path from older versions of Adobe Acrobat to Adobe Acrobat DC. Adobe Acrobat DC can be obtained from our Lab’s software download site, https://software.lbl.gov/swSoftwareDetails.php?applicationID=1. As a reminder, all Adobe products should be purchased through the Lab’s software download site.

Option 2: Use an alternative PDF reader/document signing tool
CutePDF is available for free on software.lbl.gov to support PDF generation. For users who use Adobe Acrobat as a signature tool, HelloSign is a free alternative solution to Lab employees. Windows 10 and Mac users can generate PDFs using the built-in print to PDF function. If you wish to obtain further information regarding PDF generation or HelloSign, please submit your questions to help@lbl.gov.

Acrobat EOL Inquiry

Windows CBS Log File Eating Up Disk Space

Problem

There is a known Windows 7 log file compression bug. As a result of this bug, log files replicate and grow, filling up your hard drive, affecting system performance and slowdown. Microsoft has known about the bug, but has not provided an official patch. Several users at the Lab recently have been victims of this bug and their systems are currently being addressed. If you feel your system may be affected and your hard drive is filling up, the fix provided below should address the issue.

Solution

Follow the steps:
Before you ever make any major changes to your system, always ensure you have a full and complete back up. This will enable you to restore your system if any of the fix does not work.

1. Stop the Windows Modules Installer service, by clicking Start and in the Search box type services.msc
2. Scroll down to the Windows Modules Installer service and double-click on it
3. Under Service status, click Stop, then click OK
4. Use File Explorer to go to C:\Windows\Logs\CBS. (If Windows is installed on a different hard drive, you have to go to that drive.)
5. Delete all of the files in that folder
6. For good measure, delete all the "cab" files in your Windows Temp folder, typically C:\Windows\Temp
7. Reboot

If you would like help with this process, please click the link below to request support.

**Request Help**

*This project was possible because IT identified affected systems with BigFix. To get BigFix for your computer, please visit software.lbl.gov.*

Choose a topic from the list on the left, or search for a topic.

For more general LBNL information, please use the Lab's Google Custom Search (GCS) tool or refer to the A-Z index

If you need to contribute to the IT FAQ's and find you do not have permission, contact the Help Desk and ask that you be added to the Commons faq editors group.