kindred

Security Newsletter

21 May 2018

Subscribe to this newsletter

eFail: Critical Flaws in PGP and S/MIME Tools Can Reveal Encrypted Emails

A team of European security researchers has released a warning about a set of critical vulnerabilities discovered in PGP and S/Mime encryption tools that could reveal your encrypted emails in plaintext. What's worse? The vulnerabilities also impact encrypted emails you sent in the past.

PGP, or Pretty Good Privacy, is an open source end-to-end encryption standard used to encrypt emails in a way that no one, not even the company, government, or cyber criminals, can spy on your communication. S/MIME, Secure/Multipurpose Internet Mail Extensions, is an asymmetric cryptography-based technology that allows users to send digitally signed and encrypted emails.

The EFAIL attacks exploit vulnerabilities in the OpenPGP and S/MIME standards to reveal the plaintext of encrypted emails. In a nutshell, EFAIL abuses active content of HTML emails, for example externally loaded images or styles, to exfiltrate plaintext through requested URLs. To create these exfiltration channels, the attacker first needs access to the encrypted emails, for example, by eavesdropping on network traffic, compromising email accounts, email servers, backup systems or client computers. The emails could even have been collected years ago.

The attacker changes an encrypted email in a particular way and sends this changed encrypted email to the victim. The victim's email client decrypts the email and loads any external content, thus exfiltrating the plaintext to the attacker. Being able to intercept and modify e-mails in transit is the sort of thing the NSA can do, but is hard for the average hacker. The vulnerability isn't with PGP or S/MIME itself, but in the way they interact with modern e-mail programs. Vulnerability disclosure and associated (mis)communication for eFail created a lot of heated debates within the security community.

How eFail works

Details on a New PGP Vulnerability

"Official" website

Hardcoded Password Found in Cisco Enterprise Software, Again

Cisco released 16 security advisories yesterday, including alerts for three vulnerabilities rated "Critical" and which received a maximum of 10 out of 10 on the CVSSv3 severity score. The three vulnerabilities include a backdoor account and two bypasses of the authentication system for Cisco Digital Network Architecture (DNA) Center.

The Cisco DNA Center is a piece of software that's aimed at enterprise clients and which provides a central system for designing and deploying device configurations (aka provisioning) across a large network.

The first of these flaws, and probably the easiest to exploit, is CVE-2018-0222. Cisco describes this as an "undocumented, static user credentials for the default administrative account," which is just a longer way of spelling backdoor account. Users are advised to apply software patches to remove the account as soon as possible, as there are no known workarounds that can disable it until updates can be installed.

The second vulnerability is CVE-2018-0268, which is an authentication bypass for a Kubernetes container management subsystem embedded inside Cisco's DNA Center. Last but not least there's CVE-2018-0271, an authentication bypass in the DNA Center's API gateway.

The company discovered these flaws following as part of its massive series of internal audits it started back in December 2015. The company discovered many backdoors and hardcoded accounts in the past two years as part of internal audits and has received some pretty harsh criticism for its efforts.

Read More

CVE-2018-0222

CVE-2018-0268

CVE-2018-0271

Red Hat Linux DHCP Client Found Vulnerable to Command Injection Attacks

A Google security researcher has discovered a critical remote command injection vulnerability in the DHCP client implementation of Red Hat Linux and its derivatives like Fedora operating system. The vulnerability, tracked as CVE-2018-1111, could allow attackers to execute arbitrary commands with root privileges on targeted systems.

Felix Wilhelm from the Google security team found that attackers with a malicious DHCP server, or connected to the same network as the victim, can exploit this flaw by spoofing DHCP responses, eventually allowing them to run arbitrary commands with root privileges on the victim's system running vulnerable DHCP client.

In its security advisory, Red Hat has confirmed that the vulnerability impacts Red Hat Enterprise Linux 6 and 7, and that all of its customers running affection versions of the dhclient package should update their packages to the newer versions as soon as they are available.

Read More

Security Advisory

Cutting room floor

- Moving Fast and Securing Things: Moving Fast and Securing Things
- Enhancing Pwned Passwords Privacy by Exclusively Supporting Anonymity
- Security Flaw Impacts Electron-Based Apps
- Honeypots as deception solutions: What to look for and how to buy
- Nethammer—Exploiting DRAM Rowhammer Bug Through Network Requests
- CIA's "Vault 7" mega-leak was an inside job, claims FBI
- Voice Squatting Attacks Impact Amazon Alexa and Google Home Assistants
- A bug in Keeper password manager leads to sparring over "zero-knowledge" claim
- Cell phone tracking firm exposed millions of Americans' real-time locations
- ZipperDown Vulnerability May Impact 10% of All iOS Apps
- Another severe flaw in Signal desktop app lets hackers steal your chats in plaintext
- Shadowy Hackers Accidentally Reveal Two Zero-Days to Security Researchers

#Tech and #Tools

- Google YOLO: Clever clickjacking with iframes, js and css.
- Malicious PDF Analysis Booklet by Didier Stevens
- DARKSURGEON is a Windows packer project to empower incident response, digital forensics, malware analysis, and network defense.
- Cracking Java's RNG for CSRF: Why CSRF token randomness matters
- SMB hash hijacking & user tracking in MS Outlook

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.

You can access the previous newsletters at https://news.infosecgur.us