Oracle, Gemalto Downplay Java Card Vulnerabilities

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bc8TCtNbp9w/oracle-gemalto-downplay-java-card-vulnerabilities

---

Chrome 74 Patches 39 Vulnerabilities

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_ccGM0CeoTA/chrome-74-patches-39-vulnerabilities

---

Rockwell Controller Flaw Allows Hackers to Redirect Users to Malicious Sites

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/2UbFF3PpdEA/rockwell-controller-flaw-allows-hackers-redirect-users-malicious-sites

Unexpected protection added to Microsoft Edge subverts IE security

reader comments

19 with 19 posters participating

Share this story

A researcher has uncovered strange and unexpected behavior in Windows 10 that allows remote attackers to steal data stored on hard drives when a user opens a malicious file downloaded with the Edge browser.

The threat partially surfaced last week when a different researcher, John Page, reported what he called a flaw in Internet Explorer. Page claimed that when using the file manager to open a maliciously crafted MHT file, the browser uploaded one or more files to a remote server. According to Page, the vulnerability affected the most recent version of IE, version 11, running on Windows 7, Windows 10, and Windows Server 2012 R2 with all security updates installed. (It's no longer clear whether any OS other than Windows 10 is affected, at least for some users. More about that in a moment.)

Below this paragraph in Page's post was a video demonstration of the proof-of-concept exploit Page created. It shows a booby-trapped MHT file triggering an upload of the host

computer’s system.ini file to a remote server. Page’s video shows the file being downloaded with Edge.

[embedded content]
Internet Explorer/XML External Entity Injection zero-day example video. (Loud volume warning!)
“This can allow remote attackers to potentially exfiltrate Local files and conduct remote reconnaissance on locally installed Program version information,” Page wrote. “Example, a request for ‘c:\Python27\NEWS.txt’ can return version information for that program.”

Beware of XML external entity attacks

Page’s demo is an example of an XML External Entity attack, wherein XML input is used to reference content stored on external sources. When the application parsing tainted XML doesn’t do so securely, it may disclose sensitive local information to the external entity.

Page released all the technical details and working exploit code after Microsoft told the researcher it was considering a fix but had closed the case and wouldn’t provide any status updates in the future. The vulnerability went largely unnoticed, most likely because IE has been deprecated and replaced with Edge, which by all accounts provides significantly improved security. What’s more, the two-click exploit (one click to download and another to run) requires some non-subtle social engineering of the target.

On Wednesday, security researcher Mitja Kolsek published a post warning that Microsoft had underestimated the severity of the vulnerability. The assessment was based on his discovery that Windows 10 users who open a malicious MHT file downloaded with Edge would also be attacked—and in a way that stole many more files than just the system.ini file in Page’s exploit.

Even worse, Kolsek said, Page's exploit could be improved to work more quietly and in a way that allowed the malicious file to be opened from Edge itself.

"This is clearly a significant security issue, especially since the attack can be further improved from what was originally demonstrated," wrote Kolsek, who is CEO of ACROS Security and co-founder of "micropatching" service 0patch.

Enter mark-of-the-Web

Oddly, Kolsek said he couldn't reproduce the attack when he used IE running on Windows 7 to download and then open the malicious file. While his process monitor showed that system.ini had been read, the file was never sent to the remote server.

"This looked like a classic "mark-of-the-Web" situation," Kolsek wrote. "When a file is obtained from the Internet, well-behaved Windows applications like Web browsers and email clients add a mark to such [a] file in [the] form of an alternate data stream named Zone.Identifier, containing a line ZoneId=3. This allows other applications to know that the file has come from an untrusted source—and should thus be opened in a sandbox or an otherwise limited environment."

The researcher confirmed that IE indeed put the mark-of-the-Web on the downloaded MHT file.

Kolsek then tried downloading the same file with Edge and opening it with IE, which remains the default application for MHT files. The exploit worked. After a large amount of analysis, he found the reason: Edge added two entries to the access control list:

Mitja Kolsek
James Foreshaw of Google's Project Zero vulnerability team said the entries Edge added are "capability and group SIDs for the Microsoft.MicrosoftEdge_8wekyb3d8bbwe package." After removing the second entry—SID S-1-15-2-*—from the malicious file, the exploit no longer worked. Somehow, the permission Edge was adding allowed the file to bypass the sandbox in IE.

The question was—why? A great deal more analysis using a process monitor and IDA eventually showed that the permission prevented a function called GetZoneFromAlternateDataStreamEx from reading the file's Zone.Identifier stream and returned an error. IE responded as if the file had no mark-of-the-Web and allowed the file to be sent to the remote server.

"See the irony here?" Kolsek wrote. "An undocumented security feature used by Edge neutralized an existing, undoubtedly much more important feature (mark-of-the-Web) in Internet Explorer." (It's arguable that the feature is documented here, but Kolsek disagrees.)

Despite the increased severity of Kolsek's exploit and the new insights of his research, there's no indication Microsoft intends to fix the bug soon, if at all.

"The technique described relies on social engineering and requires a user to download and open a malicious MHT file," a Microsoft representative wrote in an email. "We encourage customers to practice safe computing habits online, including exercising caution when clicking on links, opening unknown files, or accepting file transfers. More information on staying safe online is available here."

No doubt, the exploit is far from being a scary drive-by attack that takes full control of a computer. Still, in the right, ahem, *edge cases*, it might make the perfect exploit to use in targeted campaigns. Kolsek's 0patch platform has published a micropatch that he says fixes the vulnerability.

This story was updated in the second and third paragraphs to remove incorrect details about Page's PoC exploit.

https://arstechnica.com/?p=1493361

Symfony, jQuery Vulnerabilities Patched in Drupal

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/7TQpUuex83s/symfony-jquery-vulnerabilities-patched-drupal

---

Network DoS Attack on PLCs Can Disrupt Physical Processes

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/XF1PzRtnYdw/network-dos-attack-plcs-can-disrupt-physical-processes

Cisco Patches Critical Flaw in ASR 9000 Routers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/G0GDPS9psPY/cisco-patches-critical-flaw-asr-9000-routers

The wave of domain hijackings besetting the Internet is worse than we thought

Enlarge / Artist’s impression of state-sponsored “Sea Turtle” hacking campaign.
Chunumunu / Getty Images

reader comments

40 with 31 posters participating

Share this story

The wave of domain hijacking attacks besetting the Internet over the past few months is worse than previously thought, according to a new report that says state-sponsored actors have continued to brazenly target key infrastructure despite

growing awareness of the operation.

The report was published Wednesday by Cisco's Talos security group. It indicates that three weeks ago, the highjacking campaign targeted the domain of Sweden-based consulting firm Cafax. Cafax's only listed consultant is Lars-Johan Liman, who is a senior systems specialist at Netnod, a Swedish DNS provider. Netnod is also the operator of i.root, one of the Internet's foundational 13 DNS root servers. Liman is listed as being responsible for the i-root. As KrebsOnSecurity reported previously, Netnod domains were hijacked in December and January in a campaign aimed at capturing credentials. The Cisco report assessed with high confidence that Cafax was targeted in an attempt to re-establish access to Netnod infrastructure.

Reverse DNS records show that in late March nsd.cafax.com resolved to a malicious IP address controlled by the attackers. NSD is often used to abbreviate name server demon, an open-source app for managing DNS servers. It looks unlikely that the attackers succeeded in actually compromising Cafax, although it wasn't possible to rule out the possibility.

"I've also seen attributions to this name," Liman told Ars, referring to nsd.cafax.com. "The strange thing is that that name doesn't exist. There is, and, as far as I can remember, has never been, such a name in the legitimate cafax.se domain." He said the techniques involved in the March attack are consistent with the Netnod hijacking. Asked how the March attack affected Cafax customers, Liman wrote: "I don't know. I was not in a position to observe things as they happened, so I don't know what the black hats did."

The hackers—whom Talos claims are sponsored by the government of an unnamed country—carry out sophisticated attacks that typically start by exploiting known vulnerabilities in targets' networks (in one known case they used spear phishing emails). The attackers use this initial access to obtain

credentials that allow them to alter the DNS settings of the targets.

Persistent access

Short for “domain name system,” DNS is one of the Internet’s most fundamental services. It translates human-readable domain names into the IP addresses one computer needs to locate other computers over the global network. DNS hijacking works by falsifying the DNS records to cause a domain to point to an IP address controlled by a hacker rather than the domain’s rightful owner. The ultimate objective of the campaign reported by Talos is to use the hijacked domains to steal login credentials that give persistent access to networks and systems of interest.

To do that, the attackers first alter DNS settings for targeted DNS registrars, telecom companies, and ISPs—companies like Cafax and Netnod. The attackers then use their control of these services to attack primary targets that use the services. The primary targets include national security organizations, ministries of foreign affairs, and prominent energy organizations, almost all of which are in the Middle East and North Africa. In all, Cisco has identified 40 organizations in 13 countries that have had their domains hijacked since as early as January 2017.

Despite widespread attention since the beginning of the year, the hijackings show no signs of abating (which is the usual course of action once a state-sponsored hacking operation becomes well-known). Reverse lookups of 27 IP addresses Cisco identified as belonging to the hackers (some of which were previously published by security firm Crowdstrike) show that besides Cafax, domains for the following organizations have all been hijacked in the past six weeks:

- mofa.gov.sy, belonging to Syria’s Ministry of Foreign Affairs

- syriatel.sy, belonging to Syrian mobile telecommunications provider Syriatel
- owa.gov.cy, a Microsoft Outlook Web access portal for the government of Cyprus (also previously hijacked by the same attackers)
- syriamoi.gov.sy, Syria's Ministry of Interior

Attacking the foundation

In Wednesday's report, Talos researchers Danny Adamitis, David Maynor, Warren Mercer, Matthew Olney, and Paul Rascagneres wrote:

> *While this incident is limited to targeting primarily national security organizations in the Middle East and North Africa, and we do not want to overstate the consequences of this specific campaign, we are concerned that the success of this operation will lead to actors more broadly attacking the global DNS system. DNS is a foundational technology supporting the Internet. Manipulating that system has the potential to undermine the trust users have in the Internet. That trust, and the stability of the DNS system as a whole, drives the global economy. Responsible nations should avoid targeting this system, work together to establish an accepted global norm that this system and the organizations that control it are off-limits, and cooperate in pursuing those actors who act irresponsibly by targeting this system.*

Talos is calling the campaign "Sea Turtle," which it says is distinctly different and independent from the DNSpionage mass DNS hijacking campaign Talos reported as targeting Middle East organizations last November. Since the beginning of the year, most researchers and reporters believed Sea Turtle was a continuation of DNSpionage.

In an email, Talos' outreach director, Craig Williams, explained:

> *DNSpionage and Sea Turtle have a strong correlation in that they both use the DNS hijacking/re-direction methodologies to perform their attacks. However, a distinct difference is their level of maturity and capability. In DNSpionage we observed some failings, i.e. one of their malware samples was leaving a debug log. Sea Turtle has a much more mature level of playbook by attacking their ancillary targets before shifting their focus to a specific set of Middle Eastern and African victims. Overlapping [techniques, tactics and procedures] are rife due to the very closely related nature of the attacks. Without additional intelligence it would be a fair assumption to see these attacks as one of the same. Our visibility, on the other hand, makes it very clear these are two different groups.*
>
> *Talos was able to determine this distinction due to additional insights which other organizations may not have had access to. We assess, as mentioned, with high confidence that we believe DNSpionage and Sea Turtle are not related directly.*

One of the things that makes Sea Turtle more mature is its use of a constellation of exploits that collectively allow its operators to gain initial access or to move laterally within the network of a targeted organization. Cisco is aware of seven now-patched vulnerabilities Sea Turtle targets:

- CVE-2009-1151: PHP code injection vulnerability affecting phpMyAdmin
- CVE-2014-6271: remote code execution vulnerability in the GNU bash system, specifically SMTP (this was part of the vulnerabilities related to Shellshock)
- CVE-2017-3881: remote code execution vulnerability by unauthenticated user with elevated privileges in Cisco switches
- CVE-2017-6736: remote code exploit vulnerability in Cisco 2811 Integrated Services Routers

- CVE-2017-12617: remote code execution vulnerability in Apache Web servers running Tomcat
- CVE-2018-0296: directory traversal vulnerability allowing unauthorized access to Cisco Adaptive Security Appliances (ASAs) and firewalls
- CVE-2018-7600: the so-called Drupalgeddon2 vulnerability in the Drupal content management system that allows remote code execution

Talos researchers said Sea Turtle used spear phishing in a previously reported compromise of Packet Clearing House, a Northern California non-profit that manages significant amounts of the world's DNS infrastructure. In that case, as KrebsOnSecurity previously reported, attackers used the email to phish credentials that PCH's registrar used to send the Extensible Provisioning Protocol messages that act as a back-end for the global DNS system.

Once Sea Turtle hackers gain initial access to a target, they work to move laterally through its network until they acquire the credentials required to modify DNS records for domains of interest. Once the domains resolve to Sea Turtle-controlled IP addresses, the actors perform man-in-the-middle attacks that capture credentials of legitimate users logging in.

Sea Turtle uses legitimate, browser-trusted TLS certificates for the hijacked domains to hide the attacks. The certificates are obtained by using attackers' control of the domain to purchase a valid TLS certificate from a certificate authority. (Most CAs require only that a buyer prove it has control of the domain by, for instance, displaying a CA-provided code at a specific URL.) With increased control of the domain over time, attackers often go on to steal the TLS certificate originally issued to the domain owner.

VPNs? No problem

The hackers also use legitimate certificates to impersonate virtual private network applications or devices, including Cisco's Adaptive Security Appliance products. This impersonation then is used to facilitate man-in-the-middle attacks.

"By gaining access to the SSLVPN certificate used to provide the VPN portal, an individual user will be easily tricked into believing it is a legitimate service of their organization," Williams told Ars. "Sea Turtle would then be able to easily harvest valid VPN credentials and with that they would be able to gain further access to their target infrastructure."

The hijackings last anywhere from minutes to days. In many cases, the intervals were so short that the malicious domain resolutions aren't reflected in passive DNS lookups. Below are diagrams outlining the methodology:

- Steps 1 through 5.
- Steps 6-11.

Another way that Sea Turtle stands out is its use of attacker-controlled name servers. DNSpionage, by contrast, made use of compromised name servers that belonged to other entities. Sea Turtle was able to do this by compromising DNS registrars and other service providers, and then forcing them to the hacker-controlled name servers.

Secrets to success

Talos said Sea Turtle has continued to be highly successful for several reasons. For one, intrusion detection and intrusion prevention systems aren't designed to log DNS requests. That leaves a major blind spot for people who are trying to detect attacks on their networks.

Another reason is that DNS was designed in a much earlier era of the Internet, when parties trusted each other to act benignly. It was only much later that engineers devised security measures such as DNSSEC—a protection designed to defeat domain hijackings by requiring DNS records to be digitally signed. Many registries still don't use DNSSEC, but even when it is used, it's not a guarantee it will stop Sea Turtle. In one of the attacks on Netnod, the hackers used their control of Netnod's registrar to disable DNSSEC for long enough to generate valid TLS certificates for two Netnod email servers.

The previously overlooked technique allowing browser-trusted certificate impersonation has also contributed greatly to Sea Turtle's success.

Wednesday's report is the latest reminder of the importance of locking down DNS networks. Measures include:

- Using DNSSEC for both signing zones and validating responses
- Using Registry Lock or similar services to help protect domain name records from being changed
- Using access control lists for applications, Internet traffic, and monitoring
- Mandating multi-factor authentication for all users, including subcontractors
- Using strong passwords, with the help of password managers if necessary
- Regularly reviewing accounts with registrars and other providers to check for signs of compromise
- Monitoring for the issuance of unauthorized TLS certificates for domains

The report also details indicators of compromise that network administrators can use to determine if their networks have been targeted by Sea Turtle. For networks that have been compromised, undoing the damage goes well beyond restoring the

rightful DNS settings.

“There has been this huge resistance to believing how bad these compromises are,” Bill Woodcock, executive director of Packet Clearing House, told Ars. “The very first thing [attackers] do when they get in is start trying to put in a bunch more backdoors, so you really have to turn things upside down to have any reasonable assurance of security going forward. There are a lot of people who think of these things as brief incidents rather than thinking of them as ongoing campaigns.”

https://arstechnica.com/?p=1492193

Oracle Releases 297 Fixes in April 2019 Critical Patch Update

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/RTTdLI-1S4Y/oracle-releases-297-fixes-april-2019-critical-patch-update

---

Windows Flaw Exploited to

Deliver PowerShell Backdoor

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/llpGV949jbc/windows-flaw-exploited-deliver-powershell-backdoor