CYBER SECURITY THREAT ADVISORY – GOOGLE CHROME VULNERABILITY

March 27, 2019

EXECUTIVE SUMMARY

You are receiving this advisory to make you aware of a recent cyber security threat so that you can act to protect your systems and services accordingly.

A Google Chrome vulnerability has been discovered, which, if exploited, will allow the attacker to take over the device on which Chrome is installed. Google has released information noting that they have seen the vulnerability being actively exploited.

It is strongly recommended that the Google Chrome web browser be updated to the latest version to fix the issue.

HOW DOES THIS THREAT AFFECT MY ORGANIZATION?

If your organization uses Google Chrome web browser, it could be at risk of losing control over the devices that have Chrome web browser installed.

WHAT SHOULD I DO?

As soon as possible, forward this notification to your cyber security personnel or IT partners for action.

TECHNICAL DETAILS:

On February 27th, a Google Threat Analysis researcher reported a Google Chrome RCE vulnerability (CVE-2019-5786). The vulnerability affects Windows, Mac OSX, and Linux versions of Google Chrome. Google has since reported that they have become aware that an exploit for CVE-2019-5786 exists in the wild. Since then, Google released Chrome 72.0.3626.122 which contains a fix for CVE-2019-5786.

Potential attackers can employ maliciously crafted web pages designed to allow them to use previously-freed memory on a visitor's computer via the Chrome FileReader API to execute arbitrary code and take over the device or trigger a denial of service condition. Updating Google Chrome web browser to the latest version (72.0.3626.122) will fix the issue due to all previous versions being vulnerable.

Google also identified a second vulnerability impacting Windows 7, which, if exploited in conjunction with CVE-2019-5786, can amplify the adverse effect. Microsoft has issued a patch to address this vulnerability.

CYBER SECURITY THREAT ADVISORY – GOOGLE CHROME VULNERABILITY

We strongly recommend applying both security patches as soon as possible to reduce risks from attackers who may exploit these vulnerabilities.

REFERENCES

https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html
https://www.helpnetsecurity.com/2019/03/06/chrome-cve-2019-5786/
https://security.googleblog.com/2019/03/disclosing-vulnerabilities-to-protect.html
https://www.engadget.com/2019/03/07/chrome-update-zero-day/
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0808?ranMID=24542&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-RvbSyMwapMlGiWws2BMdEg&epi=je6NUbpObpQ-RvbSyMwapMlGiWws2BMdEg&irgwc=1&OCID=AID681541_aff_7593_1243925&tduid=(ir__a2bampesu9kfryazxcm9pyfc6f2xmkglez32p0oy00)(7593)(1243925)(je6NUbpObpQ-RvbSyMwapMlGiWws2BMdEg)()&irclickid=_a2bampesu9kfryazxcm9pyfc6f2xmkglez32p0oy00

FOR FURTHER INFORMATION

If you find any of the indicators of compromise (IOCs) on your networks, or have related information, please contact cyberadvice@ontario.ca

NO WARRANTY

This Cyber Advisory contains third party content and links. CS CoE does not control or maintain third party links and makes no representation or warranty that the link will still work when you click on it or the service or content is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether you want to follow any link or agree to receive or rely on any service or content that is made available to you.

Cyber Security CoE is providing information about a known threat for potential use at the sole discretion of recipients in order to protect against cyber threats. This notification is provided in order to help health care organizations enable cyber preparedness and resilience.

DEFINITIONS:

Cyber Security Threats or Incidents are events that may present risk to the security (i.e. confidentiality, availability or integrity) of an organization's information assets, systems and networks.

- Cyber Security THREAT Advice is issued when NO ACTIVE EXPLOITS are observed. Purpose of the advice: to enable organizations to prepare for and mitigate cyber threats.
- Cyber Security INCIDENT Advice is issued when an ACTIVE EXPLOIT is observed. Incident advice is time sensitive to inform partner organizations of an ongoing cyber incident for a timely response and remediation.

CYBER SECURITY THREAT ADVISORY – GOOGLE CHROME VULNERABILITY

CYBER SECURITY ADVISORY INCLUDES:

- Information about known vulnerabilities and other cyber threats and risks;
- Recommendations on mitigation activities;
- List of additional resources to help recipients better understand cyber risks and make informed decisions.