

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

July 27, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane SW
Washington, D.C. 20528-0075

The Honorable Merrick B. Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Director Easterly, Attorney General Garland and Chair Khan:

I write to request that your agencies take action to hold Microsoft responsible for its negligent cybersecurity practices, which enabled a successful Chinese espionage campaign against the United States government.

On July 12, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation published a joint advisory about a hacking campaign targeting organizations, including government agencies, that were Microsoft customers. According to press reports, “at least hundreds of thousands of individual U.S. government emails” were stolen, and the email accounts compromised include the Secretary of Commerce, the U.S. Ambassador to China, and the Assistant Secretary of State for East Asia. Rob Joyce, the director of cybersecurity at the National Security Agency, has publicly described this hacking campaign as “China doing espionage.”

Microsoft revealed in a July 14 blog post that the hack occurred because hackers had stolen an encryption key that Microsoft had generated for its identity service, Microsoft Account (MSA). MSA validates that a user is who they claim to be – for example, by verifying the password for a @hotmail.com account – and issues “authentication tokens” that confirm that a user has been validated. Consumer-facing Microsoft products, such as Outlook, verify that a token is valid by checking that a token is digitally signed using an MSA encryption key.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

Since the hackers stole an MSA encryption key, the hackers could create fake authentication tokens to impersonate users and gain access to Microsoft-hosted consumer accounts, even if a user's account was protected with multi-factor authentication and a strong password. Government emails were stolen because Microsoft committed another error. Although the stolen encryption key was for consumer accounts, "a validation error in Microsoft code" allowed the hackers to also create fake tokens for Microsoft-hosted accounts for government agencies and other organizations, and thereby access those accounts.

This is not the first espionage operation in which a foreign government hacked the emails of United States government agencies by stealing encryption keys and forging Microsoft credentials. The Russian hackers behind the 2020 SolarWinds hacking campaign used a similar technique, with a noteworthy difference. There, the targets were organizations that ran Microsoft's identity management software on their own servers, rather than relying on Microsoft's cloud service for user authentication, Azure Active Directory (Azure AD). That Microsoft software defaulted to not warning administrators when their organizations' digital identity encryption keys were removed — even though removal is a rare event strongly indicative of suspicious activity. Moreover, while Microsoft had known since 2017 that such keys could be quietly exfiltrated from customer servers running its software, it failed to warn its customers, including government agencies, about this risk.

Microsoft never took responsibility for its role in the SolarWinds hacking campaign. It blamed federal agencies for not pushing it to prioritize defending against the encryption key theft technique used by Russia, which Microsoft had known about since 2017. It blamed its customers for using the default logging settings chosen by Microsoft, and then blamed them for not storing the high-value encryption keys in a hardware vault, known as a Hardware Security Module (HSM). Instead, Microsoft used the incident as an opportunity to promote its Azure AD product. After a 2021 Senate Intelligence Committee hearing focused on the SolarWinds incident, Microsoft's President Brad Smith told the committee that "[t]hose who want the best security should move to the cloud." Microsoft's customers heard the message — it is too hard to secure these keys on your own servers, so let Microsoft do it for you. In the three years since that high-profile hacking campaign, Microsoft's cloud security business revenues have ballooned to over \$20 billion a year.

Even with the limited details that have been made public so far, Microsoft bears significant responsibility for this new incident. First, Microsoft should not have had a single skeleton key that, when inevitably stolen, could be used to forge access to different customers' private communications. Second, as Microsoft pointed out after the SolarWinds incident, high-value encryption keys should be stored in an HSM, whose sole function is to prevent the theft of encryption keys. But Microsoft's admission that they have now moved consumer encryption keys to a "hardened key store used for our enterprise systems" raises serious questions about whether Microsoft followed its own security advice and stored such keys in an HSM. Third,

the encryption key used in this latest hack was created by Microsoft in 2016, and it expired in 2021. Federal cybersecurity guidelines, industry best practices, and Microsoft's own recommendations to customers, dictate that encryption keys be refreshed more frequently, for the very reason that they might become compromised. And authentication tokens signed by an expired key should never have been accepted as valid. Finally, while Microsoft's engineers should never have deployed systems that violated such basic cybersecurity principles, these obvious flaws should have been caught by Microsoft's internal and external security audits. That these flaws were not detected raises questions about what other serious cybersecurity defects these auditors also missed.

While Microsoft certainly deserves most of the blame, the executive branch also bears responsibility. On May 12, 2021, President Biden issued Executive Order 14028, which among other things, created a Cyber Safety Review Board, whose first task would be to study the SolarWinds incident. That review never took place — the Board was subsequently directed by the Department of Homeland Security to study another hacking incident. I have repeatedly pushed CISA and DHS to direct the Board to study the SolarWinds incident, but have been rebuffed. Had that review taken place, it is quite likely that Microsoft's poor data security practices around encryption keys would have come to light, and this most recent incident might have been averted.

Holding Microsoft responsible for its negligence will require a whole-of-government effort. To that end, I request that each of your agencies take the following actions:

Director Easterly, I urge you to exercise your shared authority to direct the Cyber Safety Review Board to investigate this incident. In particular, the Board should examine whether Microsoft stored the stolen encryption key in an HSM, a best practice recommended by the National Security Agency and even by Microsoft, and if not, examine why Microsoft failed to follow its own security advice. The Board should also examine why Microsoft's negligence was not discovered during the external audits that were required to obtain certification for government use under the FedRAMP program, or during Microsoft's own internal security reviews.

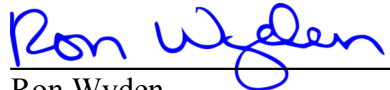
Attorney General Garland, the Department of Justice has previously pledged to “use [its] civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards.” I urge you to examine whether Microsoft's negligent practices violated federal law.

Chair Khan, I urge you to investigate Microsoft's privacy and data security practices related to this incident to determine if Microsoft violated federal laws enforced by the Federal Trade Commission, including those prohibiting unfair and deceptive business practices. In addition, Microsoft was subject to a consent decree for 20 years after a security incident with its

predecessor single sign-on product, Passport. That consent decree, which expired in December 2022, required Microsoft to “establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers” for Passport or substantially similar services. Microsoft Account, the product from which the encryption key was stolen, is Passport’s modern successor. If Microsoft’s negligent cybersecurity practices predated the expiration of the consent decree, I also urge you to take all necessary steps to hold the company responsible for any violations of that order.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator