

Netöryggisráðstefna Fjarskiptastofu 2024

Einum veikleika frá Game Over



Lyf við ADHD ófánlegt í 23 daga: „Ótrúlegt að ég skuli vera uppistandandi“



Gunnhildur Kjerúf Birgisdóttir

17. febrúar, 2022 08:08



© Mynd: Júlía Rós Atladóttir/Shutterstock

Alexander Martin

April 24th, 2024

Industry

Cybercrime

News Briefs

News



Get more insights with the
Recorded Future
Intelligence Cloud.

[Learn more.](#)

Sweden's liquor shelves to run empty this week due to ransomware attack

A ransomware attack on a Swedish logistics company has prompted warnings from the country's sole liquor retailer that its top shelves in stores around the country may be empty by the end of the week.

The directly affected company, Skanlog, is a critical distributor for Systembolaget, the Swedish government-owned retail chain with a monopoly on the sale of beverages stronger than 3.5% alcohol by volume.

Skanlog's chief executive, Mona Zuko, told newspaper [Dagens Industri](#) that the incident was a ransomware attack from a group based in North Korea. The basis on which that attribution was made is not clear.

The logistics company is so important to Systembolaget that the company's press officer, Teodor Almqvist, [warned](#) that certain beers, wines and spirits — and even paper bags — could be sold out within a few days.

All beverage categories at all stores throughout the country are affected. Systembolaget said there was no risk of "total drying out" but that certain brands were likely to disappear until deliveries started arriving again.



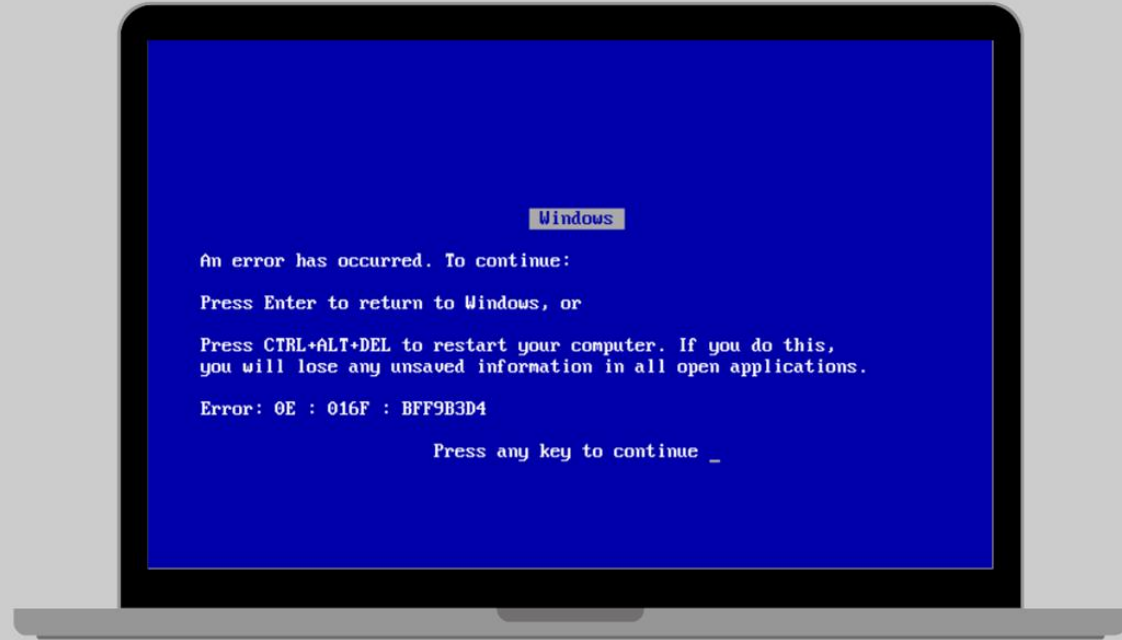
Samþykktja fyrirframgefnar
upplýsingar



“The blue screen of death”



CROWDSTRIKE



How Boeing 737 MAX MCAS works?

Maneuvering Characteristics Augmentation System is a B737 MAX anti-stall system

When MCAS activates?

- Autopilot OFF
- Flaps UP
- Too high angle of attack
- Low speed
- Steep turns
- High load factors

Stall
MCAS ACTIVATION THRESHOLD
Safe Angles

AOA SENSOR

Alpha vane which is part of AOA sensor aligns with air flow and measures the angle of attack.

If the angle exceeds the activation threshold, MCAS activates and rotates the horizontal stabilizer to push the nose down.

MCAS deactivates if the angle of attack is back to normal range or pilot overrides it manually.

EVIONICA | EVIONICA.COM



BOEING

Commercial Defense Space

737 MAX SOFTWARE UPDATE

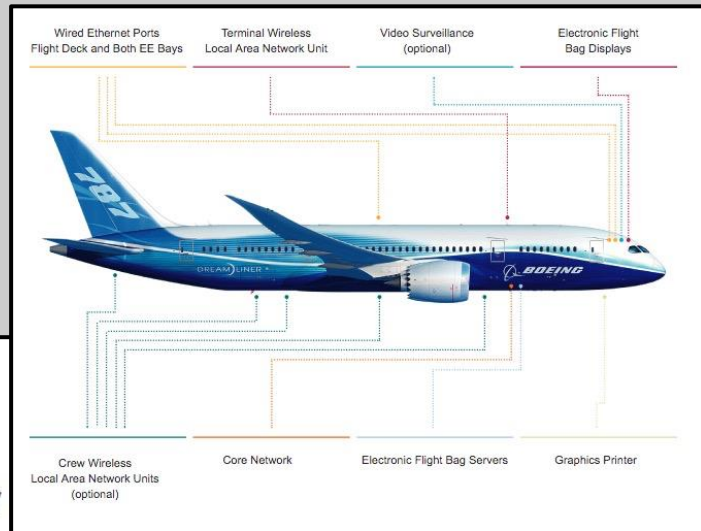
OVERVIEW TRAINING FLIGHT DECK DISPLAYS

COMMERCIAL > 737 MAX > 737 MAX UPDATE > 737 MAX SOFTWARE UPDATE



GAME
OVER

Boeing 787 Dreamliner



Index of /onsParts/airplaneCredentials

Name Last modified Size Description

Parent Directory	-	-	-
170512-204146-N7X72T.>	2018-09-17 15:15	1.0K	-
170524-155747-N7X72T.>	2017-06-01 16:35	1.0K	-
170602-210030-N7378T.>	2017-06-05 14:55	1.0K	-
170713-173901-N7X72T.>	2017-07-21 00:35	1.0K	-
170725-010650-N7378T.>	2017-08-01 18:55	1.0K	-
170801-185542-N7378T.>	2017-08-02 14:15	1.0K	-
170822-160352-N7378T.>	2017-08-26 21:05	1.0K	-
170914-153637-N7X72T.>	2017-09-24 21:05	1.0K	-
170928-211404-N7X72T.>	2017-10-20 14:05	1.0K	-
171116-033708-N7X72T.>	2018-02-02 07:25	1.0K	-
180202-032739-N7X72T.>	2018-02-12 13:05	1.0K	-
180211-104742-N7X72T.>	2018-02-19 02:25	1.0K	-
180219-212925-N7X72T.>	2018-02-20 22:15	1.0K	-
ACN4D-KEYS-0005/	2017-04-20 19:25	-	-
ACN49-KEYS-0001/	2017-04-18 01:00	-	-
BOE2F-0AS6-123C/	2016-08-16 21:34	-	-
ITL3C-APK0-0007/	2017-03-21 16:45	-	-

- **September 2018**
- **Publicly available Boeing server**
- **Google query**

Files

- **787's Core Network Cabinet Fw**
- **737's Onboard Network System Fw**
- **VM to VPN into a Boeing network**

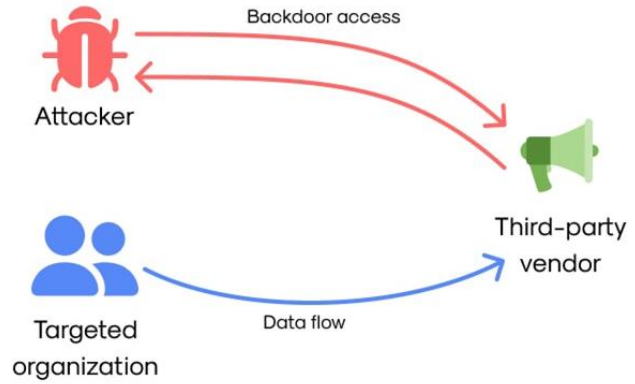
https://act-on.ioactive.com/acton/attachment/34793/f-cd239504-44e6-42ab-85ce-91087de817d9/1/-/-/-/Arm-IDA%20and%20Cross%20Check%3A%20Reversing%20the%20787%27s%20Core%20Network.pdf?utm_campaign=2023+-+IOActive+%7C+Promotions+-+blog



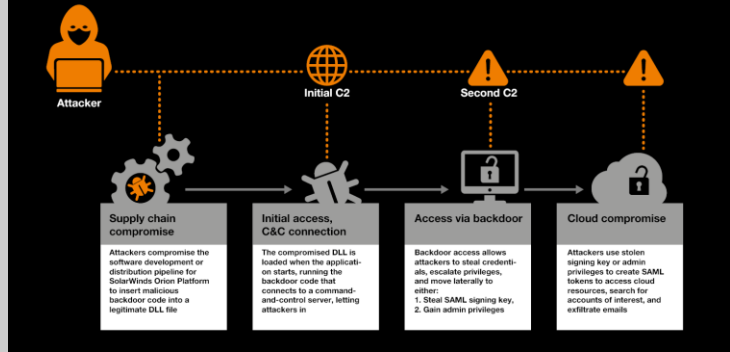
Don't be the weakest link in the security chain.

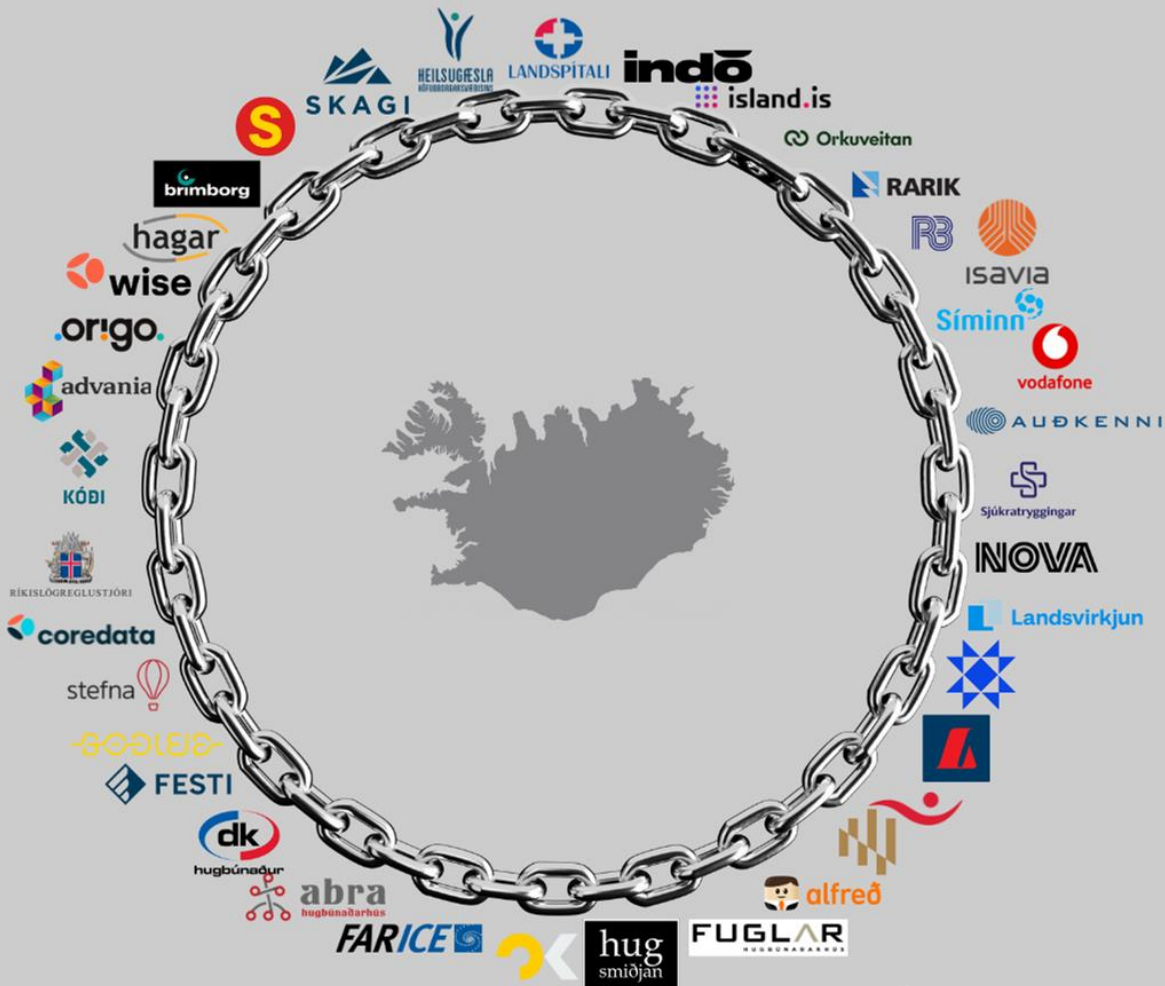


Supply Chain Attack

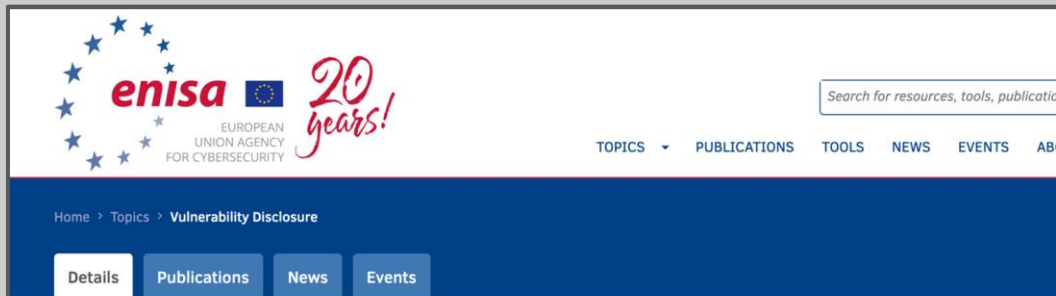


Solorigate attack High-level end-to-end sophisticated supply-chain compromise





“Coordinated Vulnerability Disclosure” (CVD) hefur varla tíðkast á Íslandi



By setting rules for identifying, fixing, mitigating, and reporting new vulnerabilities before they are exploited, CVD is crucial for protecting users and strengthening cybersecurity in the EU.



Vulnerability Disclosure

Coordinated Vulnerability Disclosure

The digital world sees constantly the discovery of new vulnerabilities. These weaknesses can leave users exposed to attacks that steal data or disrupt critical systems. Coordinated Vulnerability Disclosure (CVD) is critical to protecting users. It tries to ensure that vulnerabilities are disclosed to the public after the responsible parties developed a fix, a patch or provide mitigation measures to limit the threat posed by the exploitation of a vulnerability.



Það sem þú veist ekki að þú veist ekki

“Coordinated Vulnerability Disclosure” (CVD) hefur varla tíðkast á Íslandi

Öryggissérfræðingur



Það er veikleiki í kerfunum hjá þér!

Fyrirtæki



Takk fyrir tilkynninguna!
Veikleikinn er í hugbúnaðarvöru
sem er skrifuð af Birgja X!

Birginn



Takk fyrir tilkynninguna! Við
förum í það að búa til uppfærslu
og látum alla okkar viðskiptavini
vita af þessum veikleika svo þau
geti lagað sín kerfi!

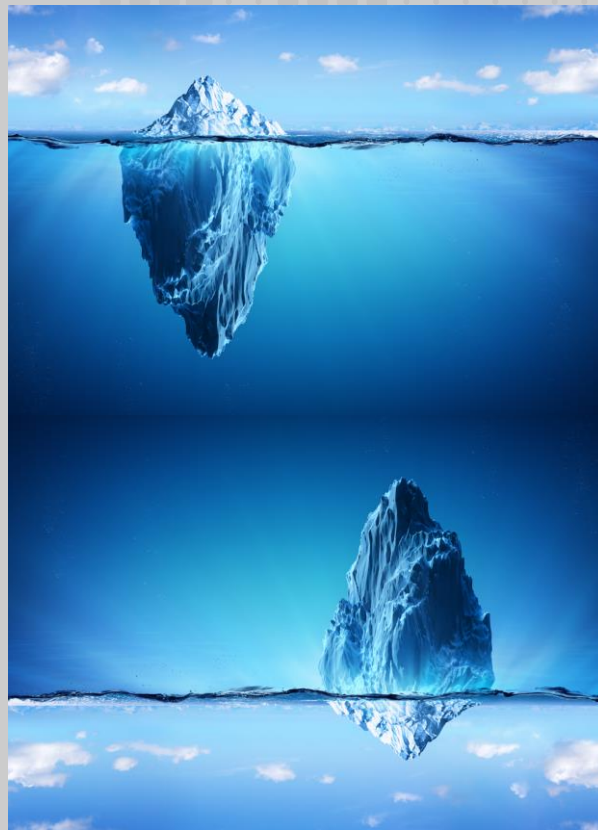
Viðskiptavinir birgjans



Viðskiptavinir birgjans laga
kerfin sín. Eftir einhvern tíma
(oft 90 dagar) er veikleikinn
birtur opinberlega svo læra
megi af honum!

95%

öryggisveikleika
voru óþekktir

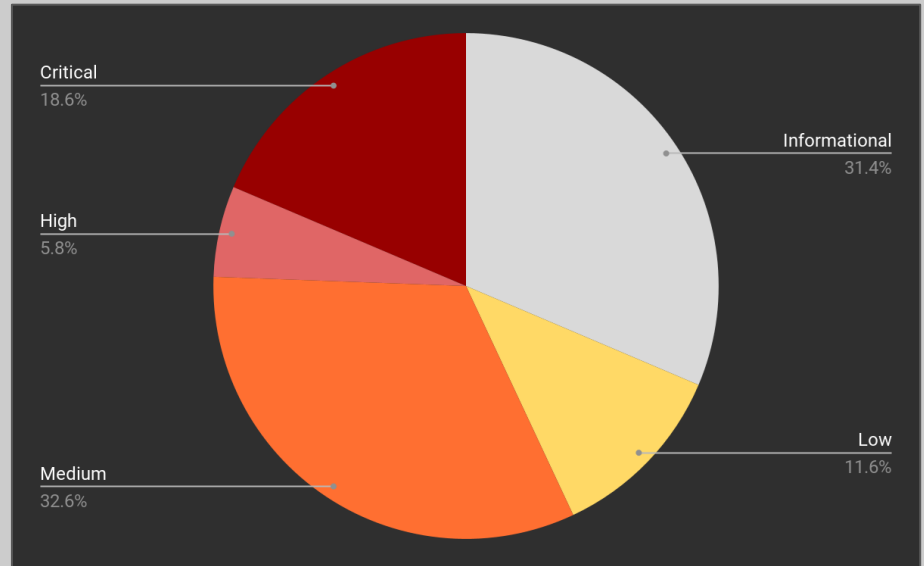


Það sem þú veist ekki að þú veist ekki

Samtals tilkynntir veikleikar hjá Defend Iceland

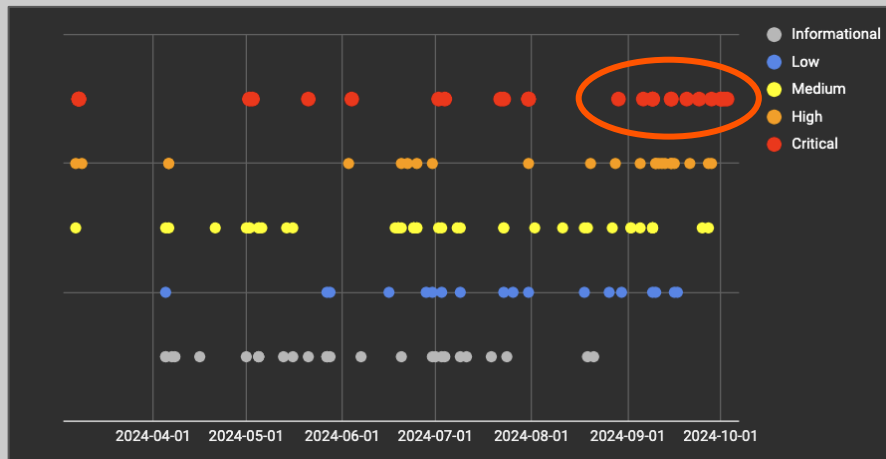
Samtals 137 staðfestir veikleikar í gegnum villuveiðigátt Defend Iceland

- 95% veikleika áður óþekktir (ekki með skráð CVE númer)
- 56% af veikleikunum flokkaðir sem 'Medium' eða hærra.
- Alvarlegustu veikleikarnir gátu leitt til alvarlegra gagnaleka eða gagnagíslaárása
- Langsamlega flestir þessara veikleika voru lagaðir mjög fljótt og engin ógn stendur af þeim lengur.



Veikleikatilkyningar yfir tímabil

- Mikil virkni innan samfélagsins
- Tilkyningartíðni eykst með hverjum mánuði.
- Metfjöldi veikleikatilkyninga bárust í September (meðtaltali 1,1 dag)
- Birgðakeðja íslensk hugbúnaðar farin að styrkjast. Dæmi um fundna veikleika í vefumsjónar kerfum, mannauðs og umsóknar kerfum, skjalastjórnunarkerfum, viðskiptakerfum (SaaS) og auðkenningarkerfum hefur jákvæð áhrif á samfélagið í heild
- Eftir stendur mikil áskorun að ná fram “Coordinated Vulnerability Disclosure” fram á Íslandi
- Fólk og fyrirtæki hrædd við orðið “veikleiki”



Öryggisvirkileiki





Takk fyrir!



Ég á LinkedIn



Defend Iceland á
LinkedIn