DARK SKY
TECHNOLOGY

MITRE Hot Topics in Supply Chain Security

Open Source Software Supply Chain Security Issues

DARK SKY
TECHNOLOGY

Finally. Trust in Open Source

MITRE Hot Topics in Supply Chain Security

Open Source Software Supply Chain Security Issues

(RC-77) Supply Malicious Taint

Risks related to the integrity of a supply (product) introduced through explicit intent, whether internally or externally driven, to violate legal/business norms to cause harm.

(RC-9) Supply Counterfeit

Risks related to the authenticity of a supply (product) introduced through explicit intent, whether internally or externally driven, to violate legal/business norms.

(RC-8) Supply Hygiene

Risks affecting the ability of a supply (product) to perform as expected. This involves characteristics related to establishing and maintaining the quality, security, resilience, etc. of the supply (product).

(RC-77) Supply Malicious Taint

(RC-162) Software Supply Chain Integrity Risks

(RC-149) Manufacturing Process Integrity Risks

(RC-154) Geopolitical Integrity Risks

(RC-153) Functional Integrity Risks

(RC-151) Logistics/Transportation Integrity Risks

(RC-152) Poor Reputation for Integrity

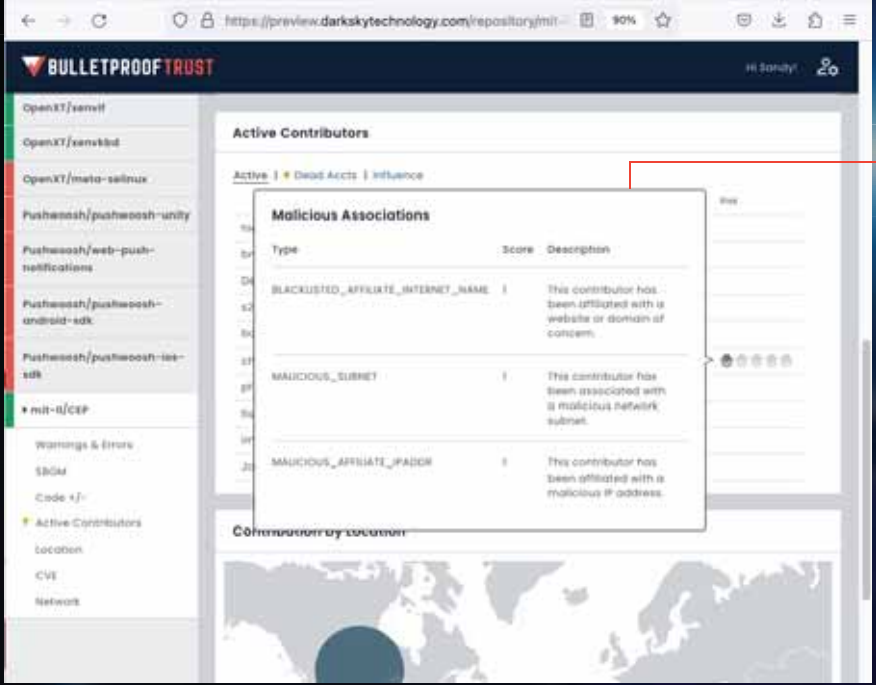
(RC-54) Packaging Integrity Risks

(RC-156) Maintenance Integrity Risks

(R

(RC-162) Software Supply Chain Integrity Risks

Risks that increase the likelihood a software supply (product) may have been tampered with because of integrity issues with supply chain management.



https://preview.darkskytechnology.com/repository/mit-

- OpenXT/xenvif
- OpenXT/xenskbd
- OpenXT/meta-selinux
- Pushwoosh/pushwoosh-unity
- Pushwoosh/web-push-notifications
- Pushwoosh/pushwoosh-android-sdk
- Pushwoosh/pushwoosh-ios-sdk
- mit-ll/CEP
  - Warnings & Errors
  - SBOM
  - Code +/-
  - Active Contributors
  - Location
  - CVE
  - Network

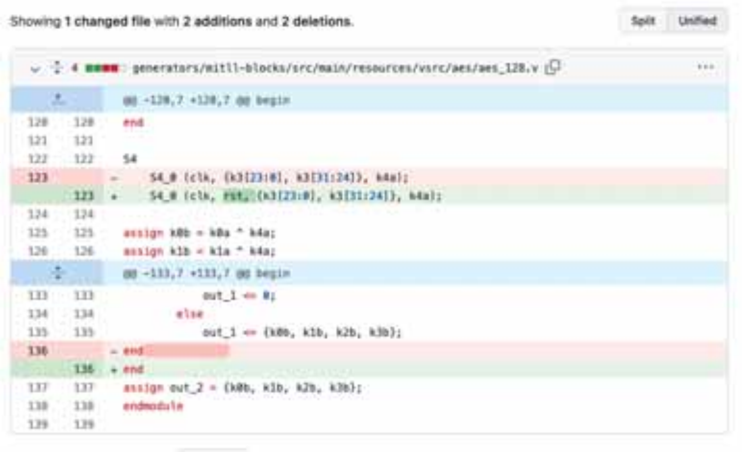
Active Contributors

Active | Dead Accts | Influence

Malicious Associations

Type	Score	Description
BLACKLISTED_AFFILIATE_INTERNET_NAME	1	This contributor has been affiliated with a website or domain of concern.
MALICIOUS_SUBNET	1	This contributor has been associated with a malicious network subnet.
MALICIOUS_AFFILIATE_IPADDR	1	This contributor has been affiliated with a malicious IP address.

Contribution by Location



Showing **1 changed file** with **2 additions** and **2 deletions.**

```
4 generators/mitll-blocks/src/main/resources/vsrc/aes/aes_128.v

@@ -120,7 +120,7 @@ begin
    end

    S4
-       S4_0 (clk, {k3[23:0], k3[31:24]}, k4a);
+       S4_0 (clk, rst, {k3[23:0], k3[31:24]}, k4a);

    assign k0b = k0a ^ k4a;
    assign k1b = k1a ^ k4a;
@@ -133,7 +133,7 @@ begin
                out_1 <= 0;
            else
                out_1 <= {k0b, k1b, k2b, k3b};
-   end
+   end
    assign out_2 = {k0b, k1b, k2b, k3b};
    endmodule

```

(RC-77) Supply Malicious Taint

(RC-149) Manufacturing Process Integrity Risks

Risks that increase the likelihood a supply (product) may have been tampered with because of inadequate manufacturing or development process integrity controls.

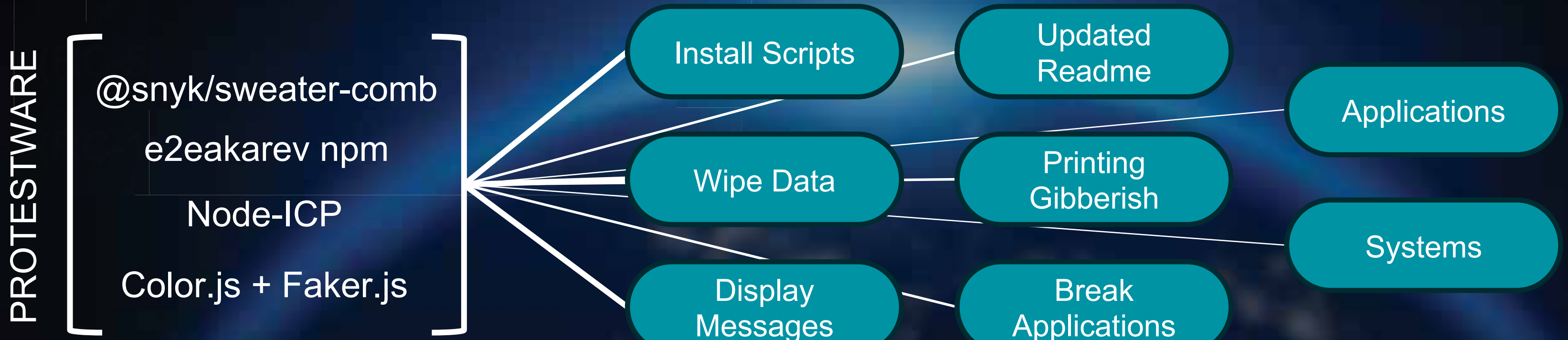
Memory Exploit

Heartbeat section of the OpenSSL cryptography and communications security package… Exposed usernames, credit card numbers, server encryption keys, everything in memory

(RC-77) Supply Malicious Taint

(RC-154) Geopolitical Integrity Risks

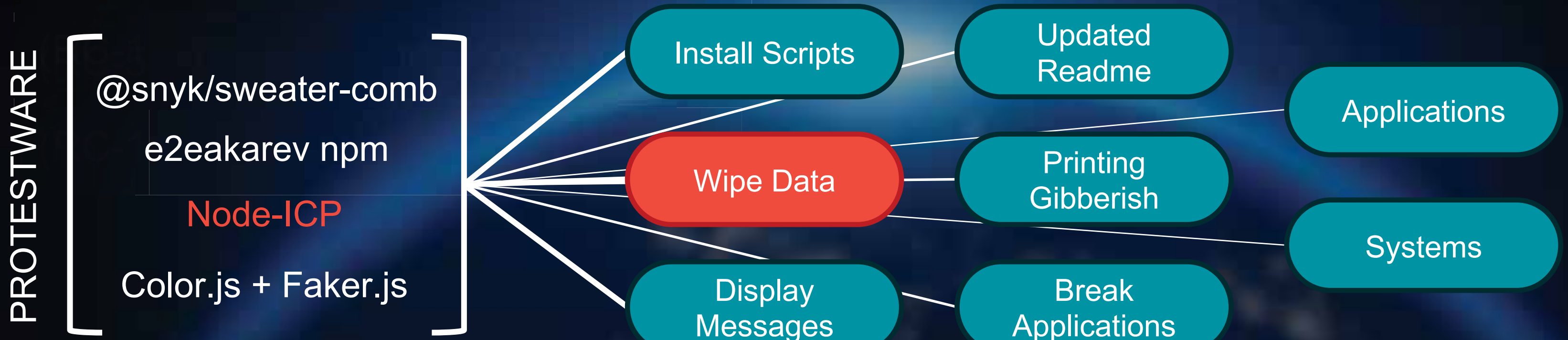
Risks that increase the likelihood a supply (product) may have been tampered with because of geopolitical conditions that negatively affect the pedigree or provenance of the supply (product).



(RC-77) Supply Malicious Taint

(RC-153) Functional Integrity Risks

Risks that increase the likelihood a supply (product) may have been tampered with because it does not perform desired functions or performs functions not desired.



(RC-77) Supply Malicious Taint

(RC-151) Logistics/Transportation Integrity Risks

Risks that increase the likelihood a supply (product) may have been tampered with because of inadequate integrity controls around the movement and transportation of the supply (product).

Phishing Campaign + Compromised Credentials = Malicious Code Posed as Legitimate Release

24 August 2022

PyPI received reports of a phishing campaign targeting PyPI project contributors…

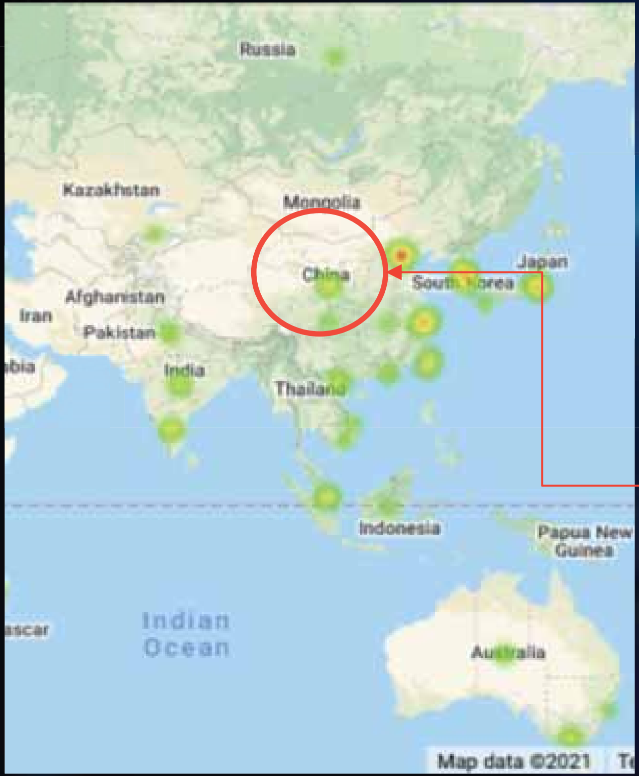
PyPI

The Official Package Index for Python

(RC-77) Supply Malicious Taint

(RC-152) Poor Reputation for Integrity

Risks that increase the likelihood a supply (product) may have been tampered with because of poor reputation for supply (product) integrity.



Top 10 Open-Source Contributors

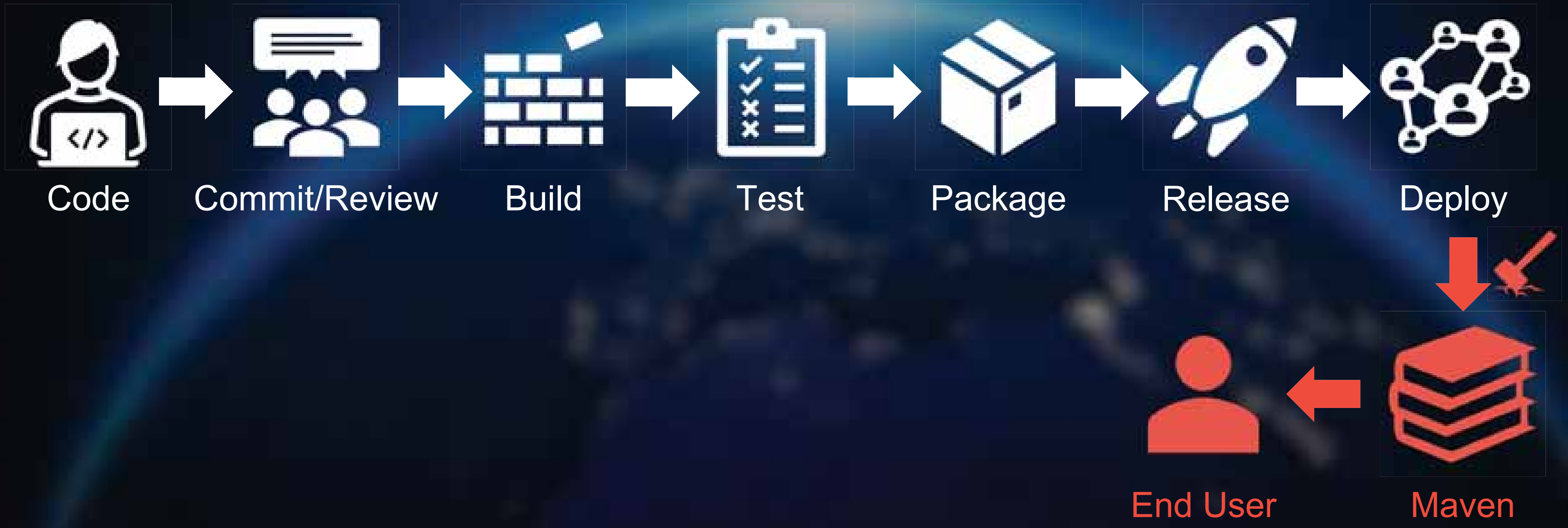
COMPANY		CONTRIBUTORS		COMMUNITY	
1.	Google	5,709	(+1,252)	11,361	(+1797)
2.	Microsoft	5,051	(+192)	10,095	(+567)
3.	Red Hat	3,127	(+361)	5,003	(+561)
4.	IBM	2,382	(+274)	5,039	(+549)
5.	Intel	2,233	(+154)	5,175	(+126)
6.	Amazon	1,231	(+381)	3,145	(+968)
7.	Facebook	1,203	(+89)	3,411	(+436)
8.	GitHub	987	(+324)	2,356	(+677)
9.	SAP	901	(+169)	1,790	(+276)
10.	Huawei	699	(+425)	1,683	(+930)

https://opensourceindex.io

(RC-77) Supply Malicious Taint

(RC-54) Packaging Integrity Risks

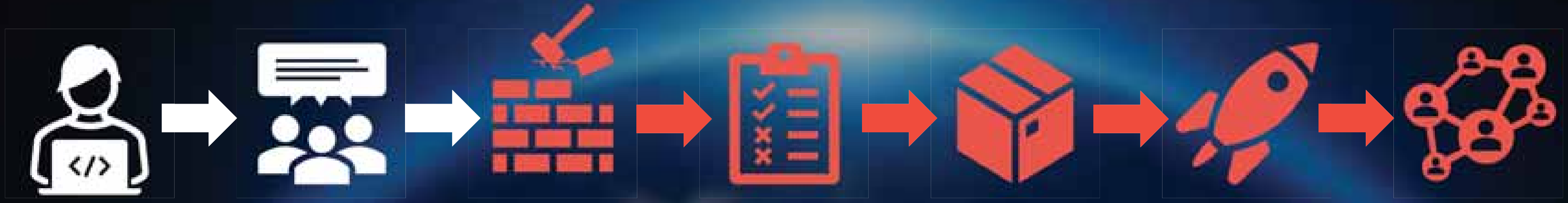
Risks that increase the likelihood a supply (product) lacks authenticity or integrity because of inadequate tamper protection or evidence of tampering with the packaging of the supply (product).



(RC-77) Supply Malicious Taint

(RC-156) Maintenance Integrity Risks

Risks that increase the likelihood a supply (product) may have been tampered with because of maintenance issues, including the update of software.



Code → Commit/Review → Build → Test → Package → Release → Deploy

CCleaner

Ultra-popular free computer cleanup tool backdoor into an auto-update inflicting over millions of computers with a backdoor.

(RC-77) Supply Malicious Taint

(RC-77) Supply Malicious Taint

(RC-162) Software Supply Chain Integrity Risks

(RC-149) Manufacturing Process Integrity Risks

(RC-154) Geopolitical Integrity Risks

(RC-153) Functional Integrity Risks

(RC-151) Logistics/Transportation Integrity Risks

(RC-152) Poor Reputation for Integrity

(RC-54) Packaging Integrity Risks

(RC-156) Maintenance Integrity Risks

(R

(RC-54) Packaging Integrity Risks

(RC-156) Maintenance Integrity Risks

Taint

(RC-127) Unsanctioned Manufacturing

(RC-126) Mislabeling

(RC-128) Copycat Manufacturing

(RC-9) Supply Counterfeit

(RC-8

(RC-127) Unsanctioned Manufacturing

Risks that increase the likelihood a supply (product) is not authentic because of manufacturing by authorized entities outside of their authorized scope.

Log4J

A powerful, widely-used open-source logging utility created by the Apache Software Foundation

Discovered in Minecraft servers…

Disclosed by Alibaba…

and posted on Twitter

Allowed remote code execution

Affected 100’s of millions of devices

68,000+ servers still at risk

(RC-9) Supply Counterfeit

(RC-127) Unsanctioned Manufacturing

(RC-126) Mislabeling

Risks that increase the likelihood a supply (product) is not authentic because the printed markings identifying the supply (product) are not as expected.

Colorama

or

Colourama

Legitimate python package called "Colorama" that redirected Bitcoin transfers to an attacker-controlled wallet.

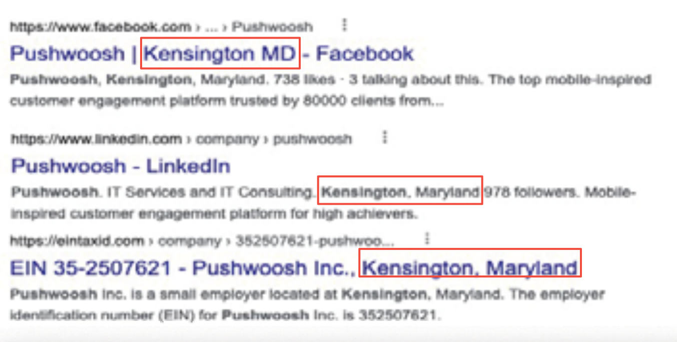
csoonline.com

(RC-9) Supply Counterfeit

(RC-128) Copycat Manufacturing

Risks that increase the likelihood a supply (product) is not authentic because of manufacturing by unauthorized entities to mimic an authentic supply (product).

The Story…



https://www.facebook.com › ... › Pushwoosh

Pushwoosh | Kensington MD - Facebook

Pushwoosh, Kensington, Maryland. 738 likes · 3 talking about this. The top mobile-inspired customer engagement platform trusted by 80000 clients from...

https://www.linkedin.com › company › pushwoosh

Pushwoosh - LinkedIn

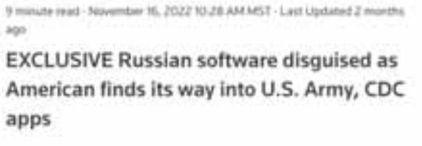
Pushwoosh. IT Services and IT Consulting. Kensington, Maryland 978 followers. Mobile-inspired customer engagement platform for high achievers.

https://eintaxid.com › company › 352507621-pushwoo...

EIN 35-2507621 - Pushwoosh Inc., Kensington, Maryland

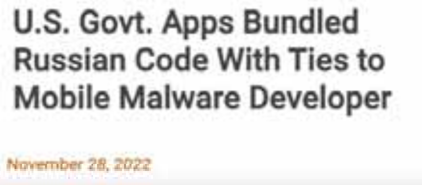
Pushwoosh Inc. is a small employer located at Kensington, Maryland. The employer identification number (EIN) for Pushwoosh Inc. is 352507621.

Our Exposure…



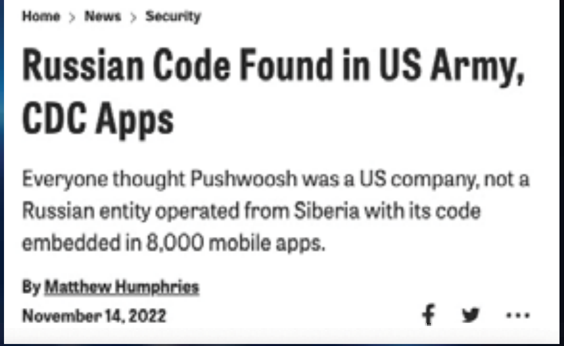
9 minute read · November 16, 2022 10:28 AM MST · Last Updated 2 months ago

EXCLUSIVE Russian software disguised as American finds its way into U.S. Army, CDC apps



U.S. Govt. Apps Bundled Russian Code With Ties to Mobile Malware Developer

November 28, 2022



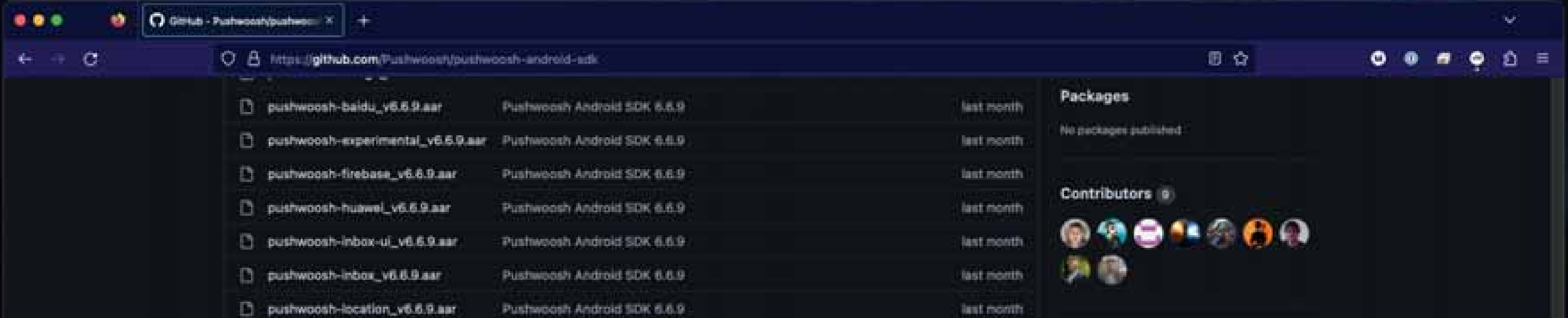
Home › News › Security

Russian Code Found in US Army, CDC Apps

Everyone thought Pushwoosh was a US company, not a Russian entity operated from Siberia with its code embedded in 8,000 mobile apps.

By Matthew Humphries

November 14, 2022



GitHub - Pushwoosh/pushwoo
https://github.com/Pushwoosh/pushwoosh-android-sdk

pushwoosh-baidu_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month
pushwoosh-experimental_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month
pushwoosh-firebase_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month
pushwoosh-huawei_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month
pushwoosh-inbox-ui_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month
pushwoosh-inbox_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month
pushwoosh-location_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month

Packages

No packages published

Contributors 9

(RC-9) Supply Counterfeit

(RC-54) Packaging Integrity Risks

(RC-156) Maintenance Integrity Risks

Taint

(RC-127) Unsanctioned Manufacturing

(RC-126) Mislabeling

(RC-128) Copycat Manufacturing

(RC-9) Supply Counterfeit

(RC-8

nterfeit

(RC-213) Supply (Product) Security Risks

(RC-201) Supply (Product) Quality Risks

(RC-8) Supply Hygiene

(RC-213) Supply (Product) Security Risks

Risks affecting the ability of a supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RC-8) Supply Hygiene

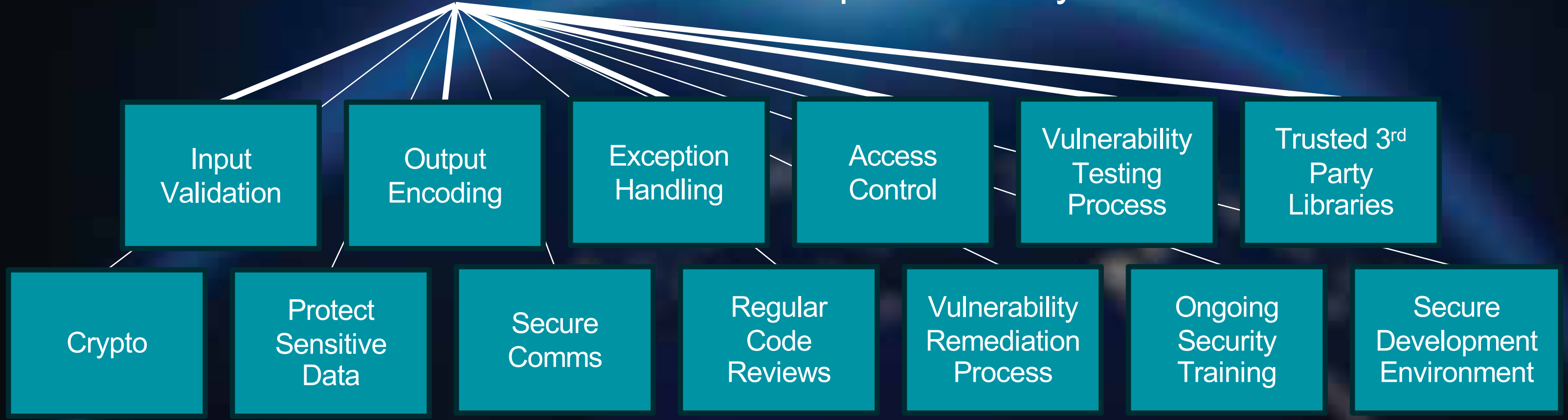
(RC-213) Supply (Product) Security Risks

(RC-201) Supply (Product) Quality Risks

Risks that increase the likelihood a supply (product) may have been tampered with because of geopolitical conditions that negatively affect the pedigree or provenance of the supply (product).

SSDLC

Secure Software Development Lifecycle



Input Validation

Output Encoding

Exception Handling

Access Control

Vulnerability Testing Process

Trusted 3rd Party Libraries

Crypto

Protect Sensitive Data

Secure Comms

Regular Code Reviews

Vulnerability Remediation Process

Ongoing Security Training

Secure Development Environment

(RC-8) Supply Hygiene

DARK SKY
TECHNOLOGY

Finally. *Trust* in Open Source

INFO@DARKSKYTECHNOLOGY.COM