# Security advisory YSA-2020-01 – insufficient data validation in yubikey-val

Published date: **2020-03-03**
Tracking ID: **YSA-2020-01**
CVE: CVE-2020-10184, CVE-2020-10185

## Update: March 13, 2020

On March 12, Yubico received a reported SQL injection vulnerability related to the YubiKey Validation Server security update issued on March 6, 2020. Our team re-reviewed the updated codebase and believes there are no known unmitigated SQL injection vulnerabilities associated with the security update.

When issuing the security update on March 6, based on several deployments and customer interactions, we implemented a minimally invasive security update to mitigate compatibility regressions. This approach was to deliver a quickly deployable fix, instead of rewriting large portions of the current YubiKey Validation Server project.

We are still focused on delivering a modern open-source project to replace the current project with expected availability in July 2020.

## Summary

Yubico received a report from LinkedIn Information Security indicating there is insufficient data validation in the open-source project for YubiKey Validation Server (git: yubikey-val). Yubico verified the issue and has made a security update available to mitigate this issue and enhance the validation of information sent to the APIs. The next major release of the YubiKey Validation Server will become available by July 2020.

This issue potentially affects developers, partners, and customers who have used a YubiKey Validation Server to build a self-hosted one-time password (OTP) validation service. The default configuration of the service only exposes the verify API, which could allow an attacker to perform a denial of service, potentially preventing legitimate authentications. Additionally, if the configuration has been modified to expose the sync API, then this vulnerability could potentially be used by an attacker to replay a previously used OTP.

## Affected Software

YubiKey Validation Server releases 2.39 and prior: available from https://github.com/Yubico/yubikey-val

## Affected Yubico devices and services

None. This advisory only pertains to the YubiKey Validation Server project. It does not affect any YubiKey Series, Security Key Series, YubiKey firmware, or YubiCloud Service.

## Customer Actions

If you are managing an implementation of a YubiKey Validation Server, update your deployment to version 2.40 of YubiKey Validation Server (available https://github.com/Yubico/yubikey-val) to mitigate this issue. Also confirm that the configuration of your service does not unnecessarily expose API endpoints.

## How to check your sync API configuration

1 Go to your configuration script (ykval-config.php)

2 Look for the following lines:

```
s['__YKVAL_ALLOWED_SYNC_POOL__'] = array(
",

",
",
aa::",
bb::",
cc::",
```

uncommented IP addresses listed in this array, then these hosts are allowed to use PI, and interact with the affected code. **These IP addresses should be limited to nodes participating in the sync pool.**

We use cookies to ensure that you get the best experience on our site and to present relevant content and advertising. By browsing this site without restricting the use of cookies, you consent to our and third party use of cookies as set out in our Cookie Notice.

Preferences Accept all

] in this array, then no hosts are allowed to use

verify, sync, resync, and revoke. By default, the IP whitelist. YubiKey Validation Server does not e verify and sync APIs. Insufficient input injection attacks. The level of impact of the SQL injection varies depending on the configuration of the YubiKey Validation Server instance. Verify performs basic validation on all fields prior to executing database queries but does not check length. An attacker could abuse this issue by submitting a large entry to be input into the database, which could cause a denial of service.

Sync does not perform consistent validation on received parameters prior to executing database queries. However, only sources that are defined in the __YKVAL_ALLOWED_SYNC_POOL__ are allowed to call the sync API, which limits the exposure of this issue. The default configuration does not define any allowed sources for the sync API, meaning all attempts to call the sync API will be denied. YubiKey Validation Server implementers may add IP addresses to the sync pool to enable syncing between multiple validation servers. An attacker with an allowed IP address could potentially use this vulnerability to replay an OTP.

## Frequently asked questions

**How do I sign up for security or product updates?**

To sign up for security or product updates via email, visit our email subscription page: https://pages.yubico.com/email_subscription.html

**Is YubiCloud affected?**

No, YubiCloud is not affected.



Yubico © 2022. All Rights Reserved.



We use cookies to ensure that you get the best experience on our site and to present relevant content and advertising. By browsing this site without restricting the use of cookies, you consent to our and third party use of cookies as set out in our Cookie Notice.

Preferences Accept all