Third-Party Software Was Entry Point for Background-Check System Hack

N nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/

Hackers broke into third-party software in 2013 to open personal records on federal employees and contractors with access to classified intelligence, according to the government's largest private employee investigation provider.

That software apparently was an SAP enterprise resource planning application. It’s unclear if there was a fix available for the program flaw at the time of the attack. It’s also not clear whether SAP—which was responsible for maintaining the application—or USIS would have been responsible for patching the flaw.

But in the end, sensitive details on tens of thousands of national security personnel were exposed in March 2014.

Assailants infiltrated USIS by piggybacking on an “exploit,” a glitch that can be abused by hackers, that was “present in a widely used and highly-regarded enterprise resource planning (‘ERP’) software package,” an internal investigation obtained by *Nextgov* found.

USIS officials declined to explicitly name the software application, saying they would let the report, compiled by Stroz Friedberg, a digital forensics firm retained by USIS, speak for itself.

The report, written in December 2014, noted: “Forensic evidence shows the cyberattacker gained access to USIS systems through an exploit in a system managed by a third party, and from there migrated to company managed systems. . . . Our findings were largely informed by a variety of logs, including, firewall logs, security event logs, VPN logs, and SAP application trace logs.”

A September 2014 letter from Stroz reported, "The initial attack vector was a vulnerability in an application server, housed in a connected, but separate network, managed by a third party not affiliated with USIS.” The reference to “SAP application trace logs” in the report indicates the third party was SAP.

During the period of the hacking operation, which began in 2013 and was exposed in June 2014, 20 to 30 new critical vulnerabilities were identified in SAP’s enterprise resource planning software.

The number of SAP vulnerabilities "would have given attackers many options to target SAP directly,” based on how USIS deployed the ERP tool, said Richard Barger, chief intelligence officer at ThreatConnect, a firm that tracks cyber threats. Barger is a former Army intelligence analyst.

It is unclear which vulnerability the intruders exploited. Defects in programs used by the government and contractors sometimes aren’t fixed for years after software developers announce a weakness.

Referencing the Stroz report, USIS spokeswoman Ellen Davis said, "the third-party contractor was hacked and the hacker was then able to navigate into the USIS network via the third party’s network."

Stroz officials deferred comment to USIS.

SAP, a major IT contractor with 50,000 customer organizations worldwide, would neither confirm nor deny allegations that assailants reached USIS through one of its systems. SAP spokesman Mat Small said in an email, "Since we don’t comment on the specifics of any customer engagement without their explicit consent, SAP is unable to make a statement on the situation.”

Addressing SAP’s response to security vulnerabilities, he added, "No company is more committed to data privacy and security than SAP, and we respond rapidly, vigorously and thoroughly when potential security risks are identified.”

The targeting of middlemen and downstream suppliers has become common in sophisticated hacking campaigns, according to researchers.

The top three sectors victimized by cyber espionage last year were professional services firms, which typically support large organizations; manufacturing; and government, according to an annual Verizon data breach investigations study released last month.

Computer snoops have learned it is easier to compromise “the partner and the third party dealing with that intellectual property than the source of the intellectual property itself," Jay Jacobs, a Verizon senior analyst and study co-author, said at the time of the study’s publication.

And PWC's most recent State of Cybercrime Survey found that only 22 percent of U.S. organizations plan incident response strategies with outside suppliers.

"Not all companies recognize that supply chain vendors and business partners . . . can have lower—even nonexistent—cybersecurity policies and practices, a situation that can increase cybercrime risks across any entity that partner or supplier touches,” according to the survey, which came out a year ago.

(*Image via wk1003mike/ Shutterstock.com*) cookie banner and remembering your settings, to log into your account, to redirect you when you log out, etc.). For more information about the First and Third Party Cookies used please follow this link.

Allow All Cookies

Manage Consent Preferences

Strictly Necessary Cookies - Always Active

We do not allow you to opt-out of our certain cookies, as they are necessary to ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts of the site will not work as intended if you do so. You can usually find these settings in the Options or Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Sale of Personal Data, Targeting & Social Media Cookies

Under the California Consumer Privacy Act, you have the right to opt-out of the sale of your personal information to third parties. These cookies collect information for analytics and to personalize your experience with targeted ads. You may exercise your right to opt out of the sale of personal information by using this toggle switch. If you opt out we will not be able to offer you personalised ads and will not hand over your personal information to any third parties. Additionally, you may contact our legal department for further clarification about your rights as a California consumer by using this Exercise My Rights link

If you have enabled privacy controls on your browser (such as a plugin), we have to take that as a valid request to opt-out. Therefore we would not be able to track your activity through the web. This may affect our ability to personalize ads according to your preferences.

Targeting cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Social media cookies are set by a range of social media services that we have added to the site to enable you to share our content with your friends and networks. They are capable of tracking your browser across other sites and building up a profile of your interests. This may impact the content and messages you see on other websites you visit. If you do not allow these cookies you may not be able to use or see these sharing tools.

If you want to opt out of all of our lead reports and lists, please submit a privacy request at our Do Not Sell page.

Save Settings

Cookie Preferences Cookie List

Cookie List

A cookie is a small piece of data (text file) that a website – when visited by a user – asks your browser to store on your device in order to remember information about you, such as your language preference or login information. Those cookies are set by us and called first-party cookies. We also use third-party cookies – which are cookies from a domain different than the domain of the website you are visiting – for our advertising and marketing efforts. More specifically, we use cookies and other tracking technologies for the following purposes:

Strictly Necessary Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts of the site will not work as intended if you do so. You can usually find these settings in the Options or Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Functional Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts of the site will not work as intended if you do so. You can usually find these settings in the Options or Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Performance Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts of the site will not work as intended if you do so. You can usually find these settings in the Options or Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Sale of Personal Data

We also use cookies to personalize your experience on our websites, including by determining the most relevant content and advertisements to show you, and to monitor site traffic and performance, so that we may improve our websites and your experience. You may opt out of our use of such cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still see some advertising, regardless of your selection. Because we do not track you across different devices, browsers and GEMG properties, your selection will take effect only on this browser, this device and this website.

Social Media Cookies

We also use cookies to personalize your experience on our websites, including by determining the most relevant content and advertisements to show you, and to monitor site traffic and performance, so that we may improve our websites and your experience. You may opt out of our use of such cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still see some advertising, regardless of your selection. Because we do not track you across different devices, browsers and GEMG properties, your selection will take effect only on this browser, this device and this website.

Targeting Cookies

We also use cookies to personalize your experience on our websites, including by determining the most relevant content and advertisements to show you, and to monitor site traffic and performance, so that we may improve our websites and your experience. You may opt out of our use of such cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still see some advertising, regardless of your selection. Because we do not track you across different devices, browsers and GEMG properties, your selection will take effect only on this browser, this device and this website.

Nextgov uses cookies for analytics and personalization. By continuing to use this site, you agree to our use of cookies. Read our Privacy Policy to find out more.