ConnectWise®

ConnectWise Control Security Evaluation Matrix

POTENTIAL VULNERABILITY	BISHOP FOX	HUNTRESS	GUIDEPOINT SECURITY, LLC	CONNECTWISE STANCE
CORS	“Both the ConnectWise Control cloud and customer instances were affected by a CORS misconfiguration, which reflected the Origin provided by incoming requests. This allowed JavaScript running on any domain to interact with both the Control cloud and customer Control server APIs and perform administrative actions, such as signing session identifiers, without the victim’s knowledge. This vulnerability enables any site, regardless of the origin, to send requests to the Control API and read the resulting response.”	“Based on our analysis, it appears the ConnectWise team mitigated the exact CORS and CSRF issue in SetAccountAttributes that was highlighted in the Bishop Fox report However, we did notice that other endpoints — like GetMessages—fail to reject external origins. We agree with Bishop Fox’s assessment that is a “High” security risk.”	"The CORS configuration effectively blocks responses from being read for requests from an external domain. Additionally, the endpoint GetMessages noted as a potential issue in the Huntress Labs blog seems to be a publicly accessible endpoint. Further, it does not seem like the information returned is sensitive information at least in this instance."	Mitigation has been put into place for the SetAccountAttributes endpoint discovered by BishopFox. The /GetScripts and /GetMessages endpoints are public by design and require no authentication to access. Therefore they are operating as designed and do not represent vulnerabilities.
CSRF	“The ConnectWise Control cloud and user instances do not implement CSRF protection. If a user with Adobe Flash or an outdated version of Chrome or Chromium visited a third-party website while authenticated to the Control application, script running on the malicious website would be able modify a user’s Control account by sending API requests, without the knowledge of the victim Control user. Neither the Control cloud service nor customer instance APIs include CSRF-prevention tokens. This is a crucial security control that, if implemented, would prevent JavaScript on other domains from sending mutable-data API requests on behalf of victim users.”	“As demonstrated in this video, Bishop Fox’s JavaScript PoC for disabling Control’s “suspicious account activity” email alerts no longer works. This appears to be a direct result of ConnectWise’s efforts to enforce CORS on the SetAccountAttributes endpoint. However, this video also highlights how it’s still possible to forge a request from an external website via the GetScripts endpoint. To provide comprehensive protection throughout Control, CSRF-prevention tokens should definitely be used. We again agree with the Bishop Fox team’s recommendation”	“The Bishop Fox report detailed a proof-of-concept JavaScript that exploited the CSRF attack against the “”/Service/SetAccountATtributes”" endpoint. Presently, executing the Bishop Fox JavaScript PoC results in a failure to send the request to the “”/Service/SetAccountAttributes”" endpoint due to the CORS settings on the endpoint. Additionally, the Huntress Labs blog post identified the “”/scripts/Service/GetScripts”" endpoint as a vulnerable endpoint to CSRF. While this is technically true, the only thing that can be done by exploiting this endpoint via CSRF would be to return the contents of the script to the user. No sensitive functionality would be exploited through conducting a CSRF attack against the “”/scripts/Service/GetScripts”" endpoint.”	ConnectWise Control provides protection from CSRF by relying on correct behavior from a users browser. It is possibe for a recently authenticated CW Control user to be lured to an attacker’s site and compromised either through an unpatched browser exploit or through an unpatched Flash plugin exploit. The /GetScripts and /GetMessages endpoints are public by design and require no authentication to access. Therefore they are operating as designed and do not represent vulnerabilities. ConnectWise acknowledges CSRF-prevention tokens as industry best practice against this type of attack and is actively planning for implementation.

As of January 30, 2020

POTENTIAL VULNERABILITY	BISHOP FOX	HUNTRESS	GUIDEPOINT SECURITY, LLC	CONNECTWISE STANCE
RCE	"The ConnectWise Control server is vulnerable to a remote code execution vulnerability. Administrative users could upload unsigned extension ZIP file containing executable code that is subsequently executed by the server. When an extension is uploaded, even if the contents are not signed, they are accessible using forced browsing and can be executed on the server. An attacker able to arbitrary execute code on a SaaS Control server may have the ability to access any resources accessible to the instance itself such as S3 buckets, EC2 instances, or other sensitive resources within the cloud environment that are accessible to the compromised server."	Pending	GuidePoint Security, LLC was able to reproduce all steps within the Bishop Fox report except for the actual Remote Code Execution. When a malicious extension is installed, and then when browsing to the reported file location, the server responds with a HTTP 404 file not found error. Additionally, the extension itself is listed within the disabled extensions and has a load error as part of the status. The load error states "Error validating signature: Signature not found". Overall, this vulnerability seems to be remediated, as the uploaded code is unavailable to the user who uploaded it, and when browsing to the code location, the application responds with a HTTP 404 error.	It was patched on 10/2/2019 in the next release which was shortly after the Bishop Fox assessment. The behavior identified by Bishop Fox was unintended and had been previously identified internally. The extension framework is an intended feature that allows Administrators in our Control partner developer program to develop and publish extensions. These extensions are meant to run with the full context of the Control server application, both in the front- and back-end. Due to this and the high degree of customizability we afford no trust to partners' instances, and therefore provide full isolation between instances to guard other cloud resources from this executing code.
Information Disclosure	"The ConnectWise Control cloud service is affected by an information disclosure vulnerability that allows an unauthenticated attacker to reveal the administrator email address and postal code of an arbitrary customer Control instance."	"Thankfully, the ConnectWise team has removed partners' email addresses and postal codes from the returned requests. With that said, it's still plausible that hackers could brute force the six character instanceId in order to determine valid IDs. They may also be able to correlate this data with the returned currentLicenseCount to build a prioritized list of targeted instances. If ConnectWise plans to use these unique IDs for looking up sensitive data, we'd suggest they crank up the ID complexity."	"The /scripts/Service/GetScripts endpoint does not return any email addresses associated with the account administrator of the instance. Further, the postal code associated with the account is no longer returned."	This was patched on 9/21/2019.

POTENTIAL VULNERABILITY	BISHOP FOX	HUNTRESS	GUIDEPOINT SECURITY, LLC	CONNECTWISE STANCE
User Enumeration	ConnectWise Control is vulnerable to a user enumeration vulnerability, allowing an unauthenticated attacker to determine with certainty if an account exists for a given username.	We have validated that Control no longer returns the X-Login-Resultheader which prevents attackers from identifying valid usernames. This security issue was publicly addressed in the Control 2019.5 release notes. Job well done ConnectWise!	"The X-Login-Result header is used to disclose if the user and/or password is valid or invalid, successfully identifying invalid user accounts from valid user accounts. The X-Login-Result header is not returned by the server. Therefore, this finding is remediated."	This was patched on 10/1/2019
Insecure Cookie Scope	"The ConnectWise Control authentication cookie, CloudAuth, is scoped to the parent domain, .screenconnect.com. When a user visits a Control instance owned by a malicious SaaS customer, the user's CloudAuth token would be sent to the malicious user's SaaS instance. Sending the CloudAuth token to all screenconnect.com subdomains may be viewed as an acceptable risk, as all machines running under that domain are operated by ConnectWise. However, in the event that a malicious SaaS user gains code execution (like the one documented in this disclosure) or is otherwise able to read the content of incoming requests, the malicious user could take over the sessions of other visiting SaaS customers."	Pending	The CloudAuth cookie is no longer present.	This was patched on 10/2/2019

As of January 30, 2020