

ESA-20180417-01

Default Unrestricted SmartServer SOAP API Access

Overview

The default configuration for a SmartServer 2 edge server enables unrestricted access to the SmartServer SOAP API. An attacker can use the SOAP API to retrieve and change sensitive configuration items such as the usernames and passwords for the Web and FTP servers. Echelon recommends that integrators update the SmartServer configuration during initial installation to restrict access to the SOAP API.

Affected Products

All SmartServer 2, SmartServer 1, and i.LON 100 products.

Vulnerability Overview

Access to the SOAP API interface for the SmartServer can be restricted by user with settings in the **WebParams.dat** file. To restrict access to the SOAP API, access to the **/WSDL/iLON100.wsdl** file must be restricted to authenticated users in the **WebParams.dat** file. By default the **WebParams.dat** file restricts access to **/forms/Echelon/***, but does not restrict access to **/WSDL/***. The default configuration gives unrestricted access to the SOAP API. An attacker can use the SOAP API to retrieve and change sensitive configuration items such as the usernames and passwords for the Web and FTP servers. Using these usernames and passwords, an attacker can access the SmartServer web user interface and can replace the SmartServer firmware binaries and modules with malicious versions to execute arbitrary code.

Risk Evaluation

The risk is high with the default settings, but can be mitigated by changing the permissions in **WebParams.dat** as described in the next section.

Mitigation

To restrict access to the SOAP API, add an **“/WSDL/*:all:everywhere”** entry under Realms in **WebParams.dat** as described in Appendix C, *Securing the SmartServer*, of the *SmartServer User’s Guide*.

With this entry, the Realms entry will look as follows:

```
(Realms)
/user/Echelon/*:all:everywhere
/WSDL/*:all:everywhere
```

Acknowledgement

Echelon thanks Daniel Crowley and IBM's X-Force Red team for reporting the vulnerabilities.

History

V1.0 (2018-04-17): Initial publication

PGP Signature

To send an encrypted communication to Echelon concerning any security vulnerability questions, reports, or issues, use the following PGP key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQENBFrCu+QBCADim1Dv1Xj+wYUMpniZM0J5Cv9VtBK95NrW3U956p6s6w/WAbBj
c52p4+qF01dmXMg6x14a8lMUDzJxfzW/at6U8HcZp+Kd8TBgmU9xLpZFcb3ey41z
KbcC39c3shL9JnERci5ObB8BhsbNAswhNn7wbpMkgLfLJltxyAYINK7T9mepO3Rp
WnecyaKT21UWTE2vo1TEB1Jx6P5luCkIHeVVrZZlQmLHY4B6dU1VN4g9ngut/LNx
Rfnu9nfwkAV5sljW6zmmB6jRSgu+vV2s6rVoyc3ATxViAQDAMMOKsIOdU7gYSOSL
uXyR1bVgOTFhhPVQO+no55z/h/SfDupXqee1ABEBAAG0CFJpY2ggS2V5iQFOBBMB
CAA4FiEEFTDZ9piFJnflLx2lFAu2dl7bl7UFAlrCu+QCGwMFCwkIBwIGFQoJCA5C
BBYCAwECHgECF4AACGkQFAu2dl7bl7VeUAf+Ik9Cqx4Xhyg0P/OMFuvWd9yWqQgk
B3zls+lyBwuwRQnUoWRfWGB/JWK4Ocf7AjDzAbHcScMuCZniY/Bq1QpuguyeD9K
/d3YM17wkW2pwHkk1xd7yHikl0g87Uedt4133YOBLU/eUeAVTFQ0QLaFLzbXICO7
h7S3vXsXTao5V2GPeY4AM1i/h3tMUeOXT0ASWCL9S7AQavKnGr8HJX1e+ikj8rVX
icRBA0xcg17aSqRUdyCFJi5W0AaKXDVJSWRz6hszF799PqS/syLqYxYSU+t1uHvd
7Qnq3gPnA+qUzUtzUTqZzMDccxW/MAeazjHik0XK4Nb7BGM8wBkhO8ZT4LkBDQRa
wrvkAQgAsvyLqmDZ+1jwslTUAWLS3sJQxAjtRywgSMxiUJgGDhGYvmOqagGrVmnD
LDS8WnplKtgPpgwKtUY1niQeYwQ0wrFvkVX7iokYKWrgBTaiJLVk3SqvGqhb4Nb
8wDLpj6TjOT2B/KqNaT8NS9WVj4VCjOm6eR2R+gM2njVDu3GI1uLDwQm3VHbJUJG
JTybM0sSUtf/ZOefZkAE0tiCbgMal7J1slCat9twU+yABLwmcFy/Fk5A+krHSLM2
k5YstWj9CBzTc+LgndTHJNK0fZk0pIVG1Jar9+1TArbPEY7e6qINlaT7BbL9/Dmd
XDyvx9bP1Xmgk3hZBfzQmr7DvOGGQARAQABiQE2BBgBCAAgFiEEFTDZ9piFJnfl
Lx2lFAu2dl7bl7UFAlrCu+QCGwwACgkQFAu2dl7bl7WORAF/eFQ4TiW0KhxizvFk
Exmkdq3wYU7ymbX5KfCy+jhkhaF8Uir6We2jJ8Ko5ndR7zCy99H8lqSMNQTqCV27
Al/3iRTKXESqzoQdtjCoihtY/ZlqYUVaY2wsaj0mHzzARPxc4EXHxqhyBoqON7uf
U8b0Nxxw6646BpPwl1LqWSNScV2t0yXijp62YzaGZZ1DN5rXWQL5yUI3O4fOWrfz
Okjbf4miRiXhmr7dhs9mK9ctNZFYMQoqgacRj7/ASyjcYoSL1M2GXXXqE7IYiB
C2olzDalPgJdurOkRenWelCj7qIjq4gAfp+WlIFjdCgqgxPGL6O1GTygWetFEETK
UzV1yg==
=mgme
```

-----END PGP PUBLIC KEY BLOCK-----